UNIVERSIDAD NACIONAL DE INGENIERÍA.
Recinto universitario "Simón Bolívar"

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN.

TRABAJO MONOGRÁFICO

"Estudio de Conectividad para PROFAMILIA, Utilizando los Servicios de Acceso Remoto a Redes"

Autores:

Br. Denis Francisco Espinoza Mendoza.

Br. José René Bonilla Santos

Tutor:

Ing. Enrique José Hernández García.

Managua, Nicaragua, Diciembre 2004.

DEDICATORIA

A Dios, a quien damos gracias por la oportunidad de trabajar juntos en esta monografía, por la vida, el tiempo y la sabiduría para terminarla.

A Nuestros Padres por su Amor y Confianza incondicional a lo largo de todos estos años que culminan con el logro de nuestras metas.

A Nuestros Amigos y Compañeros de la Universidad por su inspirador apoyo y su amistad sincera.

A nuestro tutor Ing. Enrique Hernández García por habernos guiado con sus conocimientos en el desarrollo de este tema.

A todas aquellas personas que sin mencionar valoramos especialmente por su decisivo apoyo en nuestro arduo y satisfactorio trabajo

Br. José Rene Bonilla Santos ***Br. Denis Francisco Espinoza Mendoza***

AGRADECIMIENTOS

Damos gracias a la Universidad Nacional de Ingeniería, por haber confiado en la calidad del tema que desarrollamos para nuestra Monografía, por los medios y el espacio que nos facilito para la conclusión exitosa del presente trabajo.

A PROFAMILIA, por la confianza que depositó en nosotros para la realización del presente estudio, los materiales y visitas facilitados en todo el territorio y los resultados que comprenden el presente trabajo.

A nuestro tutor Ing. Enrique Hernández García por toda la sabiduría y paciencia, con la que compartió sus conocimientos, su tiempo y su valiosa experiencia en el desarrollo de este tema.

Y a todas aquellas personas que de una u otra forma nos apoyaron en la realización de nuestro arduo trabajo.

Br. José Rene Bonilla Santos ***Br. Denis Francisco Espinoza Mendoza***

Resumen

El presente trabajo es un estudio que aborda los servicios de acceso remoto orientados a marcación Dial-up, que ofrecen los sistemas operativos de red Windows NT Server 4.0, Windows 2000 Server y Linux Suse 8.0, con el propósito de brindar una orientación y accesoria a la institución denominada PROFAMILIA al momento de seleccionar y decidir la forma mas eficiente, segura y de menor costo para implantar una extranet que funcione como base para la difusión de los servicios que ayudan a mejorar su desarrollo general.

Para realizar la implementación de un nuevo servicio se deben evaluar las opciones que mejor se adapten a las características tecnológicas, servicios de red de los usuarios remotos e internos, la calidad de los servicios, repercusiones a corto y largo plazo, costos y sobre todo el nivel de seguridad requerido por la Institución.

En la institución se realizo una breve evaluación de las principales características del entorno de red, con la ayuda de un levantamiento de datos de hardware y software que documentan tanto la estructura física de la red, organización lógica de la red, configuración de protocolos y servicios empleados.

En el primer capitulo realizamos una descripción de los antecedentes históricos de la institución así como una exploración y renocimiento de la estructura de red que posee, la cual incluye: los servicios prioritarios que corren en los servidores, los sistemas operativos de redes Cliente/Servidor que existen, caracteristicas físicas de las estaciones de trabajo como servidores y su distribución física, los dispositivos de red, topográfica y topológica de red.

Los siguientes capítulos II, III y IV, describen en los sistemas Windows NT Server 4.0, Windows 2000 Server y Linux SuSe 8.0, el servicio de acceso remoto, sus características, las infraestructuras de redes que permiten ser utilizadas para realizar los enlaces remotos, los protocolos de la capa de enlace de datos y los protocolos a nivel de LAN, los niveles de seguridad que permite el servicio y las propuestas de alternativas.

En el Capitulo V se realiza una comparación de costos de requerimiento de hardware y software que cada una de las plataformas necesita para su montaje y un estudio técnico donde se realizaron prueba de conectividad punto a punto para corroborar las normas de QoS necesarias para que la propuesta sea optima.

ÍNDICE

INTRODUCCIÓN

Uno de los problemas mas serios a los que se enfrentan las infraestructuras tecnológicas de las organizaciones o empresas de cualquier naturaleza, es su estado estático el cual obliga a quienes las utilizan permanecer en los espacios físicos donde estas se encuentran, restándoles la movilidad y la dinámica de trabajo que se requiere para realizar un mayor numero de tareas, que al final se convierten en cifras positivas o negativas que específicamente se denominan ganancias o perdidas. Con el desarrollo de los nuevos modelos globalizados y expansionistas que necesitan las instituciones y empresas para seguir teniendo permanencia en sus respectivos entornos y lograr alcanzar al mayor numero de personas que requieren sus servicios, se ha difundido el uso de tecnologías que logran expandir sus infraestructuras de manera virtual a través de las interconexiones de todos sus recursos informáticos distribuidos en cualquier lugar del mundo. Puesto que la información se ha convertido en el activo mas importante y valioso de cualquier institución para mantener estándares de calidad en sus operaciones y servicios, es imprescindible que la información siempre este a la distancia de un click.

En afamadas revistas de informáticas, se comentan sobre nuevos conceptos que están evolucionando el mundo de los negocios, como es el caso de "La era On Demand" que se entiende como convertir los procesos de negocios tradicional, en un proceso mas flexible e integrado que empieza con el acceso a Internet, la publicación de la empresa o institución en la world Wide Web y la integración de la propia empresa con todos los componentes internos y externos de la misma. Esto trae como resultado una capacidad de respuesta y adaptación rápida a los cambios en los entornos donde estas se desarrollan. En nuestro país son pocas las instituciones que cuentan con infraestructuras tecnológicas apropiadas para adaptarse a los cambios, esta condición se debe a los altos costos de implantación y mantenimiento de ellas, así como a los pocos proyectos de montar una red que permita la integración nacional e internacional. Pero este concepto de la On Demand no solo se aplica a instituciones de carácter mercantil, también se puede modelar a instituciones de otra naturaleza y de pequeño tamaño como por ejemplo PYMES o en nuestro caso PROFAMILIA, que en la mayoría de los casos son los responsables de atender las necesidades que el gobierno olvida.

PROFAMILIA es una institución que tiene como misión principal ***"Mejorar la calidad de vida de las familias Nicaragüenses, a través de la oferta de servicios médicos y educativos de atención primaria en salud con énfasis en salud sexual y reproductiva"*** dirigidos especialmente a familias de escasos recursos y rurales, beneficiando así a la población de bajos ingresos económicos. En su proceso de desarrollo ha logrado llevar sus servicios a diferentes departamentos de Nicaragua, esto la obliga a mantener niveles de calidad en sus servicios a los usuarios mas alejados de la capital.

Esta institución debe seguir con su proceso de crecimiento, por lo tanto debe apropiarse de las facilidades que ofrecen las tecnologías de la información, pero como mencionamos anteriormente esto incurre mucho en costos, es aquí donde como aspirantes a un titulo profesional en las áreas de las comunicaciones debemos ofrecerle alternativas que sean coherentes con las realidades económicas que esta presenta. En la actualidad ellos poseen clínicas departamentales que atienden cantidades considerables de usuarios, y que usan como único medio de comunicación e interrelación entre si, un simple servicio de mensajería que les proporciona un ISP a través de una línea de telefonía analógica común. Consideramos que esto es un sistema de poco provecho para su plan de expansión y desarrollo, que no concuerda con el concepto de la On Demand e incurren en más gastos que beneficios.

El propósito de este trabajo estará dirigido a brindarles una alternativa de integración como institución en donde el resto de sus oficinas o clínicas remotas puedan comunicarse con facilidad y tengan mayores alcances a recursos que agilicen sus actividades, tomando en consideraciones el sistema operativo de red que existe actualmente, los recursos de red que tiene en existencia, así como sus alcances presupuestarios para implantar una alternativa de comunicación que se base en el uso del protocolo mas difundido para las conexiones de llamada por marcación, nos referimos al PPP por considerarse la adaptación mas acorde a sus necesidades y que les permite la flexibilidad de usarlo en tiempos específicos. Las alternativas se extraerán de los sistemas operativos Windows NT Server 4.0, Windows 2000 Server y Linux SuSe 8.0 por ser plataformas que cuentan con servicios de comunicación vía Dial - Up.

OBJETIVOS

Objetivo General

- ***Realizar un Estudio de Conectividad entre la oficinal central de PROFAMILIA y sus clínicas regionales, basado en los servicios que proporcionan los SOR (NT Server 4.0, 2000 Server y Linux Suse) para realiza Conectividad Remota.***

Objetivos específicos

- ***Realizar una breve documentación del entorno actual de red y del proceso actual que usa la institución para comunicarse con sus clínicas regionales.***

- ***Definir los puntos de configuración para habilitar el servicio de acceso remoto en los sistemas operativos de red, teniendo en cuenta como punto de partida la plataforma actual.***

- ***Determinar y proponer elementos de hardware más recomendados para una futura implantación del sistema de comunicación en estudio.***

- ***Determinar la mejor alternativa de SOR (Windows NT Server 4.0, Windows 2000 Server y Linux Suse 8.0) para implantar el servicio de acceso remoto de acuerdo a su entorno de red.***

JUSTIFICACIÓN

Con el estudio de conectividad de conectividad remota vía telefónica, se podrán obtener resultados que serán utilizados para realizar una evaluación técnica y financiera entre el sistema de comunicación actual y la alternativa propuesta en el trabajo investigativo.

Este estudio tiene la finalidad de integrar las estaciones de trabajo y los recursos de la Organización logrando cambiar las actividades administrativas locales limitadas de la red a una administración centralizada de los recursos y usuarios que accedan a la misma, permitiendo el control de las estaciones remotas, la actualización diaria de las bases de datos y la coordinación inmediata de los usuarios por medio de mensajería interna. Obteniendo una conexión segura, eliminando agentes externos (ISP) en el proceso de comunicación a excepción de la red telefónica pública y mejorando la privacidad en la transmisión de datos; además de minimizar los costos que resultan de mantener el sistema actual entre las clínicas regionales y la Oficina Central. El nuevo proceso de comunicación será punto a multipunto entre clínicas regionales y Oficina Central mejorando la seguridad en la transferencia de datos.

Los resultados de la presente tesis serán la base técnica y metodológica para que la institución pueda migrar de un sistema actual que se limita al servicio de mensajería a un sistema de comunicación que permita a los usuarios remotos acceder a bases de datos, mensajería, Internet y otros recursos, por tanto esto traerá un incremento en el flujo general de la información de la institución y un mayor rendimiento de ésta con respecto a la calidad de los servicios que brinda a sus usuarios. El propósito es incorporar una visión más corporativa en donde los usuarios remotos puedan de forma ágil y segura acceder a los servicios de la red, como si se encontraran ubicados localmente, mejorando la adaptabilidad de la institución a cambios tecnológicos.

Capítulo I:

PROFAMILIA

Capítulo I: PROFAMILIA

1.1 Antecedentes

PROFAMILIA, es organismo no gubernamental sin fines de lucro, nació en Nicaragua el 3 de julio d 1970 con el nombre de Asociación Demográfica Nicaragüense (ADN); posteriormente pasa a denominarse Asociación Pro-Bienestar de la familia nicaragüense, con personería Jurídica propia, según Diario Oficial de la Gaceta No.87, el 10 de mayo de 1989.

Desde su fundación ha estado afiliada a la federación internacional de planificación familiar (IPPF); a partir de 1991 su principal donante y proveedor de asistencia técnica ha sido la Agencia de los Estados Unidos para el desarrollo Internacional (USAID).

En sus inicios incursiono en el campo de la salud sexual y reproductiva (SSR), con énfasis en la planificación familiar (PF), funcionando con dos clínicas en Managua y una red de promoción comunitaria en las regiones del pacifico y central del país. A partir de 1992, inicia un proyecto de Expansión y Regionalización de sus clínicas y servicios de salud, creando siete clínicas nuevas, lo que permitió proyectarla en el ámbito nacional.

En 1998, se pone en marcha un nuevo proyecto con el propósito de diversificar los servicios más allá de los tradicionales (SSR/PF), desarrollar un proceso de auto-sostenibilidad e incursionar en el mercado Social de anticonceptivos, y se proyecto la apertura de dos clínicas más, que iniciaron operaciones en el periodo 1999-2000.

Posteriormente al fenómeno del huracán Mitch en octubre del 1998, PROFAMILIA recibió apoyo de Comercial Market Strategies (CMS), con fondos de USAID para desarrollar nuevos proyectos de atención a la emergencia en municipios y construir seis nuevas clínicas en las zonas más afectadas, las cuales iniciaron la prestación de servicios en el año 2001. Estas clínicas han permitido experimentar nuevas modalidades de presentación de servicios de salud e incrementar la presencia de la Asociación en todo el país.

1.2 Distribución Nacional

Actualmente, PROFAMILIA se caracteriza por brindar servicios médicos a través de una red de 20 clínicas de atención integral distribuidas en los departamentos del país; cuenta además con 11 clubes juveniles, un programa con más de 600 promotores comunitarios y un programa de Mercadeo Social.

Figura 1.1: Distribución Geográfica de las Clínicas de PROFAMILIA

Tabla 1.1: Distribución de las clínicas de PROFAMILIA en todo el país

REGIÓN	*CLÍNICAS*
I (NORTE)	*Estelí* *Ocotal* *Someto* *Jalapa*
II (OCCIDENTE)	*Chinandega* *León*
III (MANAGUA)	*Ciudad Jardín* *Monseñor Lezcano* *Nueva Vida* *Tipitapa*
IV (SUR)	*Masaya* *Granada* *Rivas*
V (CENTRO SUR)	*Juigalpa* *Boaco*
VI (CENTRO NORTE)	*Matagalpa* *Jinotega* *Sébaco* *Río Blanco*
VII (ATLÁNTICO)	*Bluefields* ** En esta región, no existe ninguna conexión*

Para contribuir con el funcionamiento operativo de la institución, se instaló hace 6 años una red en la Oficina Central que consta de tres equipos servidores que atienden las necesidades de las 48 estaciones de trabajo locales y permiten la recepción de correo electrónico proveniente del exterior a través del enlace que les proporciona el ISP. Con los

proyectos de auto-sostenibilidad las clínicas regionales reconocieron la necesidad de tener un sistema computarizado para administrar, guardar su información y tener una comunicación con la red de la Oficina Central. La comunicación es proporcionada por un servicio de mensajería a través de Microsoft Exchange en la parte del servidor y como cliente de mensajería Eudora. Las clínicas regionales utilizan un cliente Eudora y el servicio de mensajería ofrecido por su ISP correspondiente.

1.3 Exploración del Entorno de Red

1.3.1 Plataforma de servidores

La red de PROFAMILIA posee conexión con el mundo exterior a través de los servicios de IFX, las clínicas regionales reciben los servicios a través de IBW, estos proveedores de servicio de Internet representan un costo considerable para la institución. La red cuenta con tres servidores detallados a continuación:

Servidor	Características	S O	Servicios
UNISYS (Bosht_221)	Procesador PRO 200 MHZ, RAM de 64 MB PC-100, Disco Duro 4 GB	WinNT 4.0	SQL Server
*COMPAQ PROLIANT (Probackup)	Procesador Pentium III 1.3 GHZ, RAM de 256 MB, Disco Duro 18 GB	WinNT 4.0	SQL Server
COMPAQ PROLIANT (servidornt)	Procesador Pentium III 1.3 GHZ, RAM de 256 MB, Disco Duro 18 GB	WinNT 4.0	Proxy Server, MS Exchange, Server DHCP, Server WINS, SSH (Security Shell), Internet Information Server

Tabla 1.2: Característica de los Servidores de PROFAMILIA

Los servidores están instalados en la Oficina central. Los servidores UNISYS y *COMPAQ PROLIANT son utilizados como servidores para datos y el tercer servidor es un COMPAQ PROLIANT, se utiliza como servidor de Correo y acceso a Internet.

1.3.2 Plataforma de estaciones clientes

El entorno de los sistemas operativos que posee la institución es una combinación de diferentes versiones de sistema Microsoft Windows y sistemas de otros fabricantes. Este entorno esta cambiando lentamente hacia una estandarización (Microsoft Windows 2000 profesional), para aumentar la centralización de la administración de los recursos y servicios, disminuir costos de mantenimientos de los sistemas, brindar mayores beneficios al usuario final y prepararse para una futura migración (Windows 2000 Server) de los servidores de dominio.

Nota: ***Una descripción detallada de todos los equipos y sistemas operativos de la institución se encuentra en la sección ANEXOS.***

1.3.3 Equipos de Interconexión de Red

Estos equipos de interconexión tienen la siguiente configuración física:

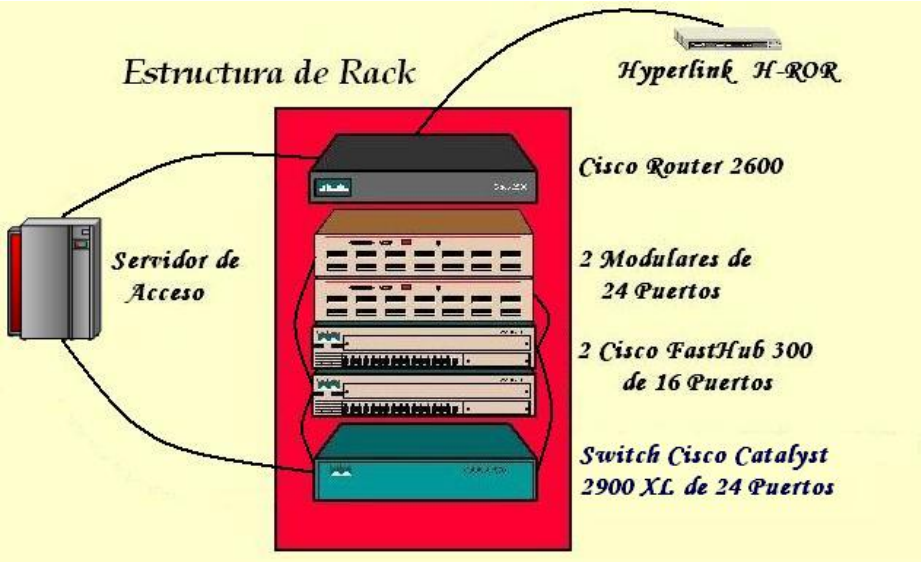


Figura 1.2: Interconexiones en el Rack

Cant.	Modelo	Características
1	**Hyperlink H-ROR**	Puente Wireless para conexiones punto a punto, maneja un rango de Frecuencia de 2400 a 2483 MHz, técnica de modulación IEEE 802.11b en secuencia directa de espectro expandido, Protocolo de acceso medio CDMA/CA, un conector de antena de prioridad reversa TNC macho y un conector Ethernet RJ-45, operación de 11 Sub Canales y un Data Rate de 11 Mbps
1	**Router Cisco 2600**	Los routers Cisco 2600 se puede elegir entre interfaces Ethernet, Token Ring y LAN Ethernet 10/100 con detección automática. Además, cuentan con dos ranuras para tarjetas de interfaz WAN (WIC), módulos de red y AIM, Consola auxiliar de 115,2 Kbps máxima, Frecuencia de 47/64 Hz. Integración multiservicio de voz y datos, Servicios de acceso analógico y digital por acceso telefónico, Acceso a VPN y VLAN. Procesador Motorola MPC860 40 MHz (Cisco 261X), 4 a 16 Mb (32 Mb máx. en Cisco 262x), DRAM de 24 a 64 MB,
2	**Patch Panel**	Para empotrar en Patch panel, de 24 puertos RJ-45 para la distribución de la red. Categoría 5e de alta densidad
2	**FastHub 300 Cisco**	100 Base TX, de 16 Puertos con modulo de expansión interno con conectores de 9 pines DB-9 Macho y conectores estándar RJ-45, operatividad en humedad entre 10 y 85 % sin condensación, compatibilidad IEEE 803.2 Clase II se Baja repetición y compatible con 100 Base T (100 Base TX y 100 Base FX), Velocidad de lectura de 100Mbps,
1	**Switch Cisco Catalyst 2900 Xl**	Dispositivo de agregación de 24 puertos con autosensado 10 base 100 Fast Ethernet y 2 Slots de Expansión de alta Velocidad para tener 250 VLANS, con un ancho de banda de 100 Mbps, compatible con IEEE 802.1, presenta una capacidad de memoria 4MB DRAM

Tabla 1.3: Características Técnicas de los equipos de interconexión

1.3.4 Distribución Lógica de los Equipos de la Red

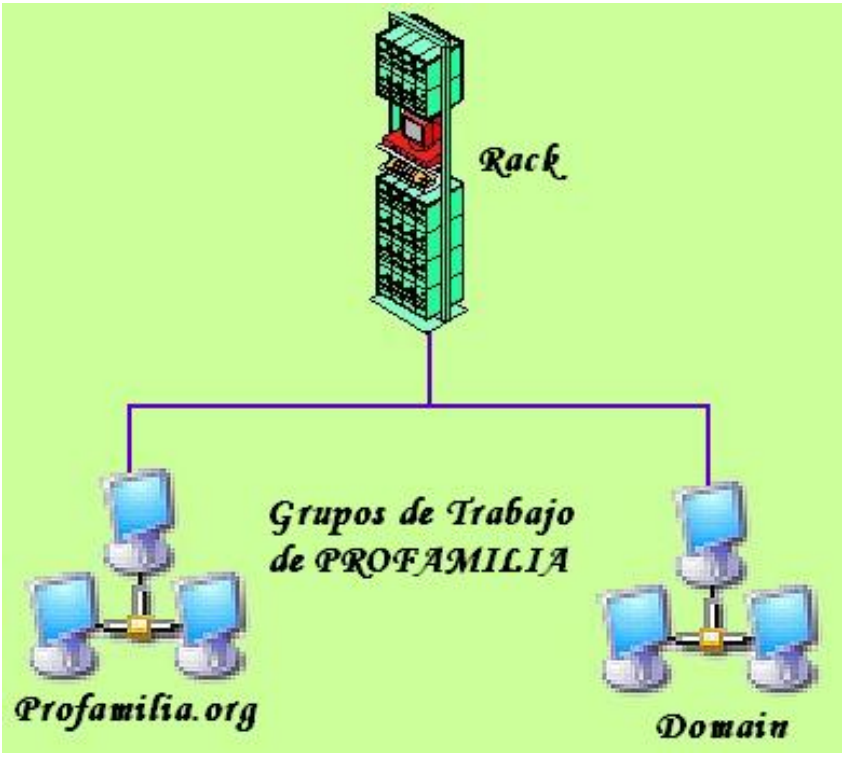


Figura 1.3: Grupos de trabajos LAN en PROFAMILIA

La LAN está compuesta por 3 servidores NT y 48 estaciones de trabajo, dividida en dos grupos de trabajo de acuerdo a la plataforma que corren los equipos de PROFAMILIA, los cuales son:

- **Profamilia.org:** Las estaciones están bajo el sistema operativo Windows 2000 Profesional. Con excepción de los tres servidores que están bajo Windows NT 4.0 Server.

- **Domain:** Las estaciones de trabajo están bajo Plataformas de Windows 95A y 95B, Windows 98 y 98Se, Windows Millenium y OSX.

1.3.5 Diagrama Físico de Interconexión de Red

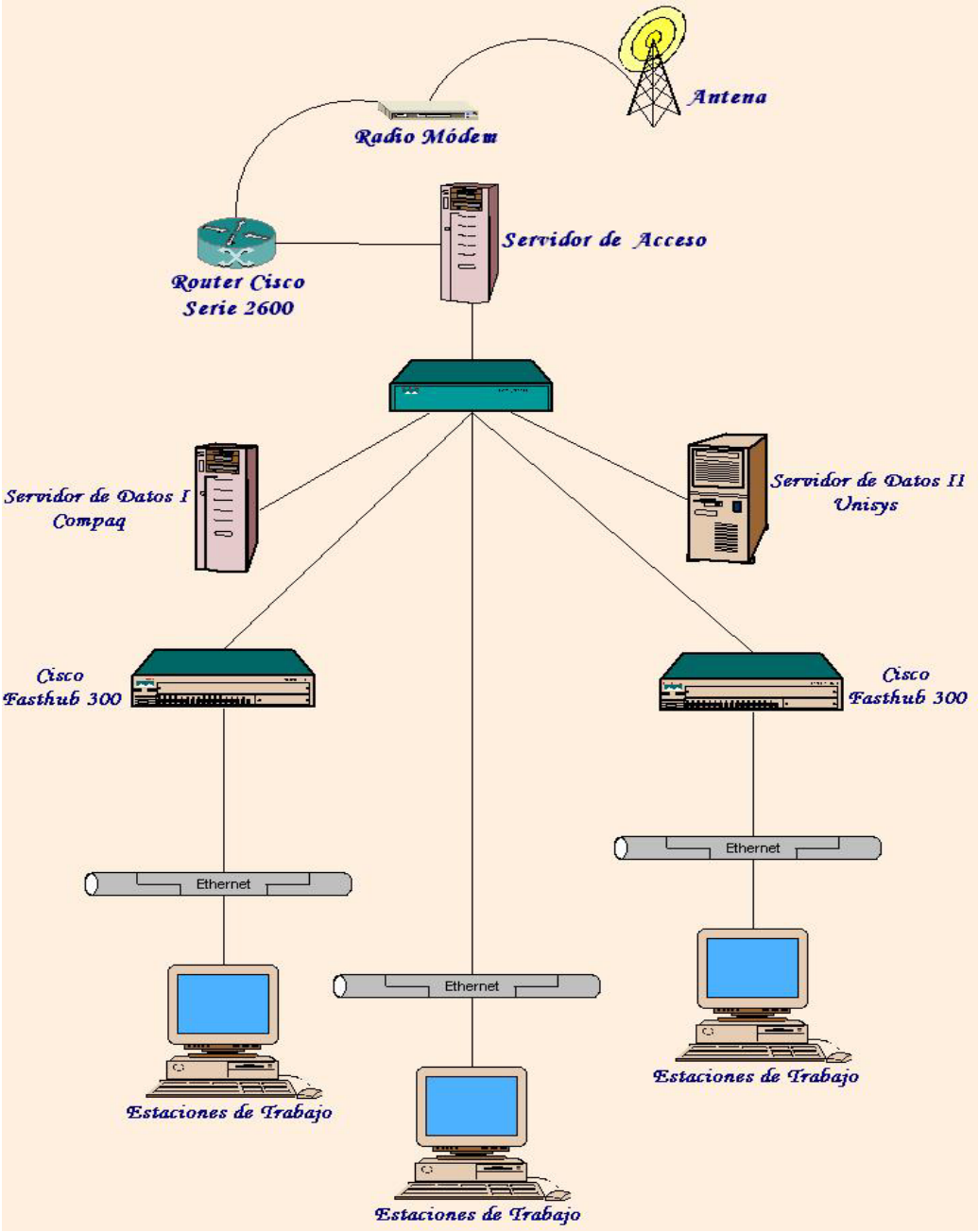


Figura 1.4: Interconexión Física de la LAN de PROFAMILIA

1.4 Forma de Comunicación

La Oficina Central accede a Internet a través de un enlace de Microondas provisto por IFX (ISP), la cual es captada por la antena y decodificado por el radio módem, este transmite la señal acondicionada para ser acoplada al Router (Cisco serie 2600), en donde se realiza

una filtración de paquetes para luego transmitir los paquetes entrantes a la red por medio del servidor de acceso que es un Proxy, delimitando así el entorno DMZ[1] de la red.

1.4.1 Proveedores de servicio de Acceso a Internet (ISP) de PROFAMILIA

ISP	Usuarios	Servicios	Conexión
IFX	Oficina Central	- Internet	Microondas.
IBW	Clínicas Regionales	- Correo - Internet	Telefónica

Tabla 1.4: Proveedores de Internet (ISP)

PROFAMILIA necesita estar en contacto con sus clínicas departamentales y lo logra a través del servicio de correo, este intercambio de información es utilizado para realizar estudios, estadísticas y para conocer el rendimiento de los servicios brindados por la institución. El flujo de dicha información sigue el siguiente esquema:

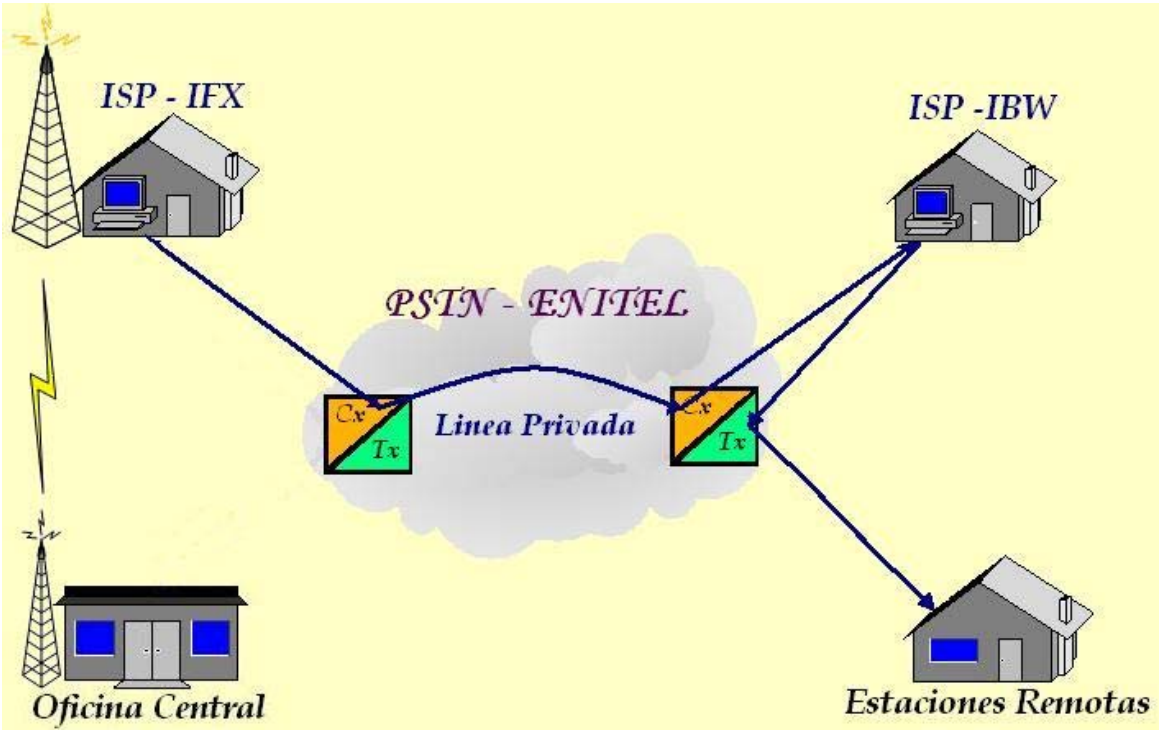


Figura 1.5: El proceso actual de flujo de la información entre la Oficina Central y Clínicas Regionales

1 MDZ (zona desmilitarizada) es una red que permite la conexión a Internet a una red privada, mientras se sigue manteniendo la seguridad de dicha red (Guía de Implantación - Windows 2000 Server).

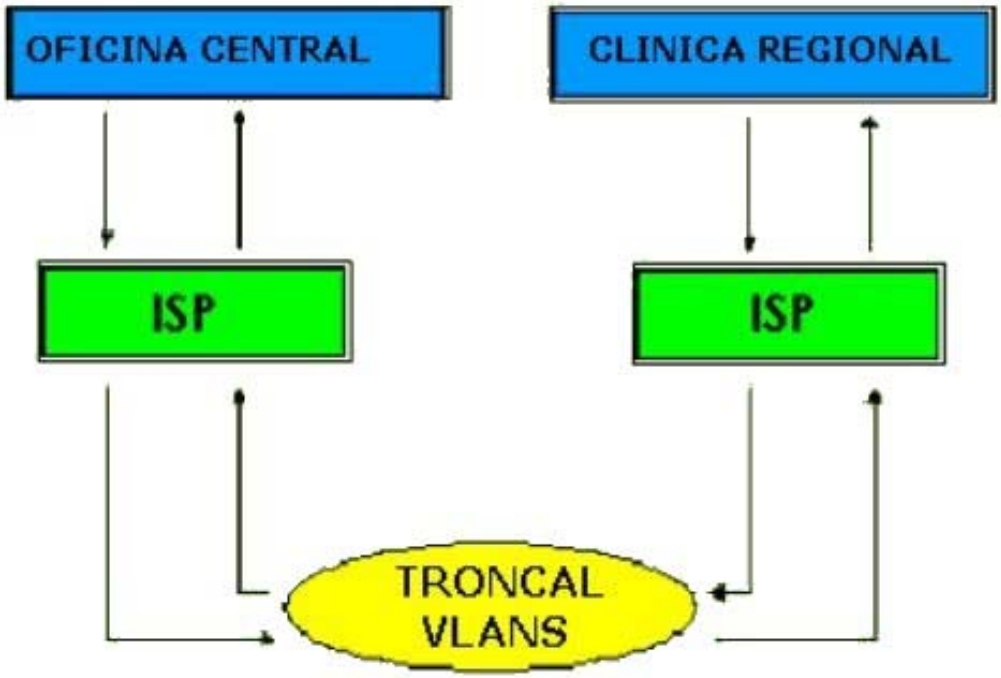
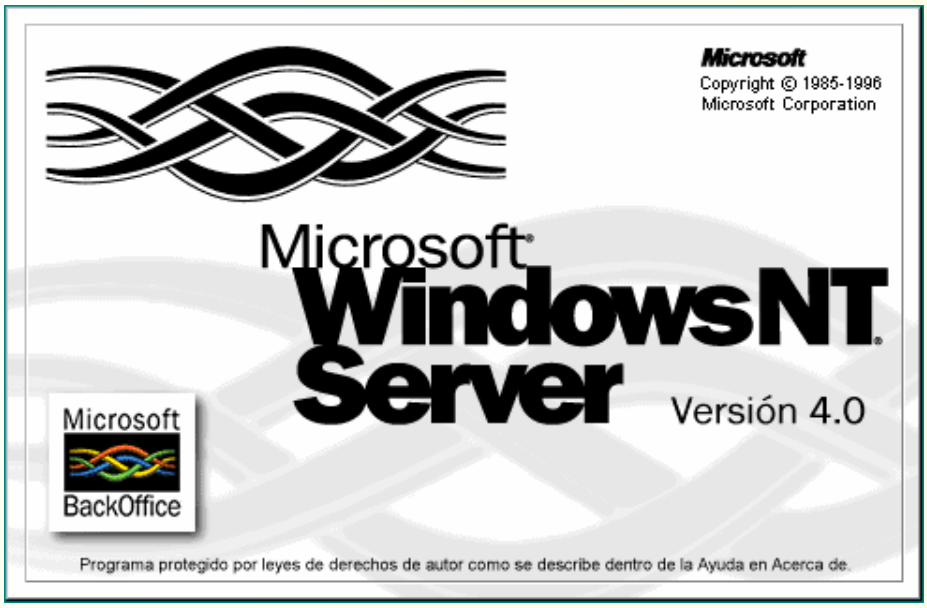


Figura 1.6: Esquema de Comunicación y Flujo de Información Entre la Oficina Central y Clínicas Regionales

PROFAMILIA contrata los servicio de dos ISP's, estos proveedores de servicios de Internet son: IFX que permite el acceso a Internet a la Oficina central e IBW brinda servicio de mensajería y acceso a Internet a las Clínicas Regionales. Cuando una clínica quiere enviar algún tipo de información hacia otra clínica o a la Oficina central, lo hace por medio de la conexión que tiene con el ISP. El flujo de información es bidireccional, de las clínicas regionales hacia el ISP que le presta el servicio, este se encarga de enviar a través del un troncal Vlans (troncal virtual) que une los ISP's, este lo recibe y lo reenvía hacia la oficina central, y viceversa.

Con excepción de la clínica de la región atlántica, todas las clínicas tienen conexión con la oficina central a través de servicios de ISP telefónico para el intercambio de información.



Capítulo II:

Propuesta De Conectividad Ras A Través De Windows NT Server

Capítulo III: Propuesta De Conectividad Ras A Través De Windows NT Server

2.1 Servicio Acceso Remoto (RAS).

Definición: Permite conectar un computador a una red remota que se encuentra en distinta ubicación geográfica. El servicio de acceso remoto trabaja bajo el modelo cliente/ servidor, y es uno de los servicios más usados para aprovechar la infraestructura WAN (Wide Área Network) de algunas redes.

2.1.1 Facilidades del Servicio

Un servidor RAS, permite:

- Que los clientes puedan conectarse por medio de líneas telefónicas analógicas, digitales o líneas X.25 a redes remotas.
- Después de haberse establecido la conexión, las líneas se vuelven transparentes al cliente y el cliente puede acceder a los recursos de la red como si fuera un computador local de la red.
- Un servidor RAS Windows NT 4.0 puede atender 256 conexiones simultáneas.

Con servicio RAS, Windows NT puede actuar como un rauter o como Gateway. Windows NT proporciona un Gateway NetBIOS para que los clientes remotos puedan alcanzar recursos NetBIOS, como servicios de archivos e impresiones de la red.
La arquitectura RAS de Windows NT tiene capacidad de enrutamiento IP (Intenet Protocol) e IPX (Internet Packet Exchange). Un servidor RAS que tiene instalado el enrutamiento IP e IPX puede realizar las siguientes funciones:

- Actuar como enrutador para enlazar redes LANs y WANs.

Conectar LANs que tienen diferentes topologías, como Ethernet y Token Ring.

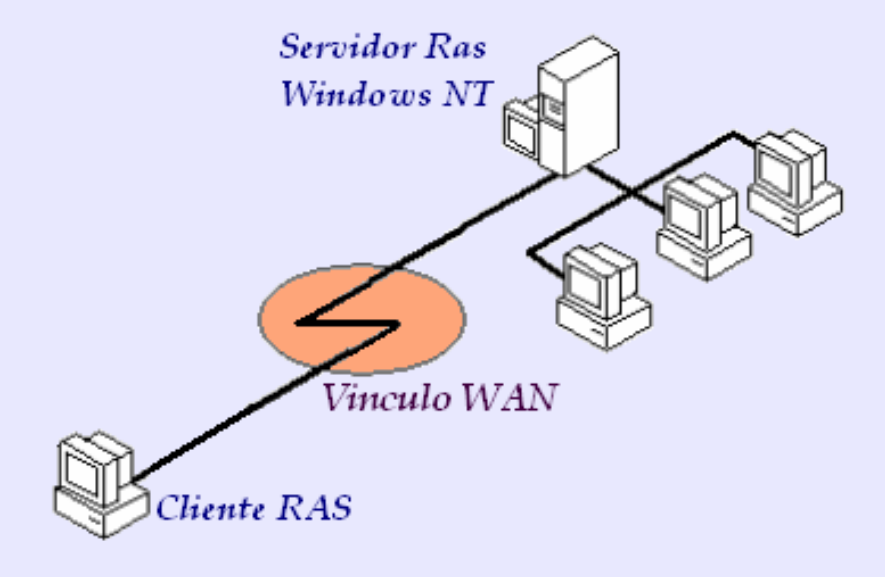


Figura 2.1: Conexión RAS

2.2 Infraestructuras WAN

Las infraestructuras de redes WAN que se pueden utilizar para implementar el servicio RAS que viene con Windows NT son: PSTN[2] (Public Switched Telephone Network), X.25[3] , ISDN (Integrated Service Digital Network).

- **Redes PSTN (Public Switched Telephone Network):** Red de Telecomunicación de tecnología analógica que proporciona un servicio de telefonía básica que transmite frecuencias mínimas para distinguir la voz humana. Útil para establecer las conexiones remotas de clientes RAS al servidor RAS, mediante módems que cumplen estándares del CCITT (Comité Consultivo Internacional para la Telefonía y Telegrafía) para estos propósitos.
- **Redes X.25:** Redes que usan la tecnología denominada conmutación de paquetes. En este tipo de redes se aumenta la velocidad y la calidad de la comunicación debido a sus características de enrutamiento de los paquetes que se transmiten sobre ella.
- **Redes ISDN (Integrated Service Digital Network):** La Red Digital de Servicios Integrados, es una nueva tecnología de red pública de telefonía que supera a su

2 Para profundizar sobre PSTN, consulte: Roger L, Freeman. Fundamentals of Telecomunications, 1ra ed. Wiley interscience, 1999

3 Para encontrar mas información sobre X.25 y ISDN en STALLINGS, W. Comunicaciones y redes de computadoras, 5ta ed. PRENTICE HALL IBERIA, Madrid, 1997

versión anterior PSTN por tener una infraestructura digital. Para utilizar servicios tipo RAS sobre esta red, es necesario que los clientes remotos y sus servidores utilicen adaptadores ISDN, como interfase de conexión entre los HOST y la red digital de servicios integrados.

2.3 Protocolos utilizados por el RAS

El servicio RAS de Windows NT, soporta dos tipos de protocolos:

- Los que Transmiten datos sobre redes LANs: TCP/IP, NWLINK IPX/SPX y NetBEUI
- Los que Transmiten datos sobre redes WANs, para acceso remoto sobre Windows NT son SLIP, PPP, PPTP.

Ya que Windows NT soporta estos protocolos LANs, puede integrarse con redes Microsoft, UNIX, Novell NetWare que usan el protocolo PPP y SLIP que son anteriores a este sistema operativo.

2.3.1 Protocolo SLIP (Serie Link IP)

Es usado para tener conexiones punto a punto. Este protocolo tiene limitaciones que le han costado su vida útil:

- Requiere una dirección IP estática, los servidores RAS no pueden utilizar servicio DHCP (Dynamic Host Configuration Protocol) o WINS (Windows Internet Name Service).
- Es un protocolo que no permite detección o corrección de errores.
- Solo reconoce direcciones IP y por lo que los extremos de los enlaces deben saber por adelantado la dirección IP de computador al que se van a conectar.
- Solo soporta TCP/IP.
- La transmisión del password al momento de autenticarse no se encripta, por lo que es muy fácil de atacarlo con programas Crakers.
- Este protocolo no es un estándar aprobado de Internet.

2.3.2 PPP[4] (Point-to-Point Protocol)

- Es una mejora de las especificaciones SLIP.
- Es un estándar que proporciona un método para el envió de datos sobre enlaces punto a punto.
- Proporciona soporte para varios protocolos tales como Apple Talk, DEC DECnet, TCP/IP, IPX y NetBEUI.
- Posibilidad para incrementar la velocidad de transmisión de datos a través de la combinación de múltiples enlaces físicos que actúan de forma lógica como un solo enlace.

2.3.3 PPTP (Point to Point Tunneling Protocol)

- PPTP es usado por clientes RAS cuando quieren acceder vía Internet a servidores RAS, creando una VPN (Virtual Private Network).
- Usando este protocolo el cliente primero establece una conexión a Internet, luego establece la conexión de Internet con el servidor RAS y se crea un túnel virtual entre ellos, permitiendo seguridad en la comunicación.

Las conexiones con este tipo de protocolo se dan de dos maneras, que varían únicamente en el tipo de acceso que tenga el cliente como el servidor para conectarse al Internet. Es decir, que las conexiones entre uno y otro extremo se pueden dar de forma directa cuando ambos tienen una interfase conectada a Internet ó de manera indirecta porque algunas de las partes necesitan un ISP (Proveedor de Servicio de Internet) para conectarse a Internet. Cuando un cliente remoto usa una red PSTN, RDSI o X.25, el cliente establece una conexión PPP con el servidor RAS sobre la red conmutada. Después que la conexión es establecida, los paquetes PPP son enviados sobre la conexión conmutada hacia el servidor RAS para ser enrutado a la Intranet. Pero cuando se usa el protocolo PPTP en lugar de tener una conexión conmutada para enviar los paquetes PPP, se usa el protocolo TCP/IP para enviar los paquetes PPP hacia el servidor RAS sobre una WAN

4 Mas detalles sobre el PPP, consulte la RFC 1661

virtual. Las ventajas que provee este protocolo en las plataformas Windows NT, son entre otras:

- Bajos costos en establecimiento de la comunicación, considerando que si el acceso a Internet es proporcionado por un ISP, el acceso remoto a la red es menos costoso que hacer una conexión telefónica vía módem marcando un número de llamadas a larga distancia.
- Bajos costos en el hardware, debido a la sencillez del enlace. Solo se necesita un ISP y el resto es configuración del servicio.
- La seguridad de la comunicación que proporciona PPTP, es soportada por el encriptamiento de los datos que viajan a través de un túnel sobre el Internet. Los datos enviados por este protocolo son paquetes PPP encapsulados.

2.4 Seguridad

RAS soporta niveles altos de seguridad, ya que las llamadas entrantes de usuarios remotos tienen que autenticarse antes de permitirle acceder a los recursos de la red.

2.4.1 Seguridad Integrada con el Dominio

Windows NT proporciona una amplia seguridad en toda una red a través de un modelo de Logon (registrarse). Este modelo de seguridad elimina la necesidad de duplicar cuentas de usuarios a través de múltiples servidores de la red.

Lo anterior facilita la administración, porque los usuarios pueden hacer Logon remotamente con la misma cuenta de usuario que utilizan cuando se encuentran físicamente en el lugar donde esta instalada la red, es decir: pueden mantener sus privilegios y permisos dentro y fuera del lugar donde esta instalada la red.

Para poder conectarse a un servidor RAS, el usuario RAS debe tener una cuenta valida en el dominio y tener los permisos de los servicios de acceso remoto para realizar llamada entrante.

2.4.2 Autenticación Encriptada y Proceso de Login

Este servicio permite elegir entre diferentes métodos de autenticación, unos más complejos que otros, pero con el mismo propósito de asegurar que entidades externas no puedan descifrar los datos que se transmiten sobre el enlace.

Los tipos de autenticación que se permiten en una conexión RAS son CHAP (Challenge Handshake Authentication Protocol), SPAP (Shiva Password Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol). Además del uso de cifrado de los datos utilizando el algoritmo de encriptación RSA Data Security Incorporated RC4.

2.4.3 Auditoria

En Windows NT se puede habilitar la auditoria de las conexiones RAS, para tener un monitoreo de los procesos de conexión y poder resolver problemas que pudieran surgir. Las actividades que puede ser auditada, son las siguientes:

- ***Conexiones rechazadas.***
- ***Desconexiones con éxito.***
- ***Retrollamadas con éxito.***
- ***Desconexiones debidas a picos en las líneas.***
- ***Tiempo de finalización de la identificación.***
- ***Errores en las líneas.***

Es posible agregar mayores niveles de seguridad a los servicios RAS, a través de la conexión de un equipo computador (Host) entre el cliente y el servidor RAS, como por ejemplo un servidor RADIUS[5] (Remote Authentication Dial-In User Service). Cuando este tipo de seguridad se establece, el cliente RAS debe autenticarse y autorizarse en el equipo intermedio para poder acceder al servidor RAS.

5 El protocolo RADIUS se encuentra documentado en las RFC's 2138 y 2139. Buscar en anexos figura del modelo de referencia OSI, mostrando en que capa de este modelo trabaja el protocolo RADIUS.

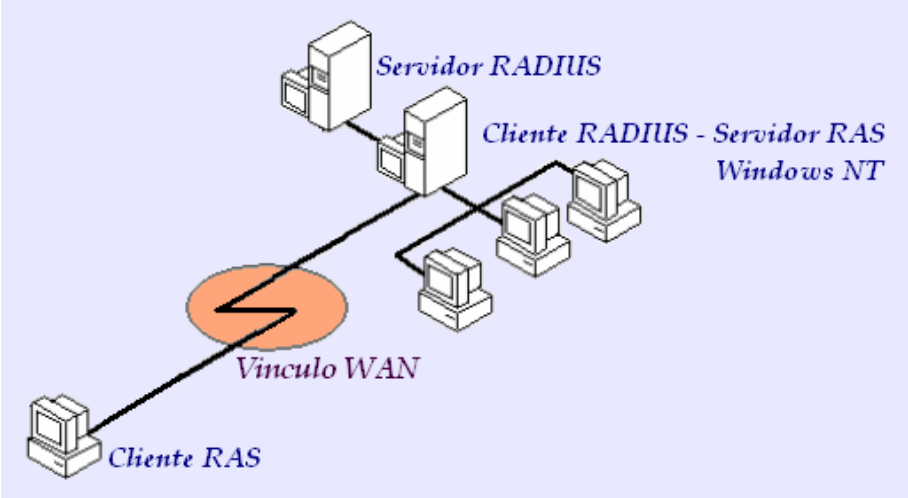


Figura 2.2: Conexión RADIUS

2.4.4 Regreso de llamada

El servicio RAS puede configurase para operar con devolución de llamada, es decir, cuando un cliente inicia una llamada al servidor RAS, este último cuelga la llamada y a continuación, él es quien realiza la llamada al cliente RAS al número telefónico que hizo la llamada inicial (el servidor tiene configurado el número al cual regresar la llamada). Este mecanismo produce un ahorro de los costos de llamada por parte de los clientes RAS.

Debe tenerse en cuenta que con la variedad de métodos de ataques a las redes, este mecanismo puede ser engañado al tener acceso a la línea telefónica. Como ultimo aspecto sobre los servicios de acceso remoto que proporciona Windows NT Server, hay que mencionar la actualización que Microsoft hizo a este servicio y que lo llamaron

2.4.5 Enrutamiento y Servicio de Acceso Remoto (RRAS)

Actualización a RRAS

RRAS sustituye tanto al Encaminador Multiprocolo como a RAS. Aunque las mejoras más significativas se concentran en las posibilidades de encaminamiento de Windows NT, RRAS también incorpora interesantes avances con respecto a RAS. La siguiente lista enumera algunas de las características más sobresalientes de RRAS:

- El encaminamiento IP incluye las versiones 1 y 2 de RIP (Routing Information Protocol) y el protocolo OSPF (Open Shortest Path First).
- Es posible administrar el encaminamiento IPX y su Protocolo de Anuncio de Servicios (SAP).
- El encaminamiento telefónico por petición permite que la LAN se conecte a una red remota como Internet a través de conexiones telefónicas basadas en módems ó en RDSI.
- Routing and RAS Admin, herramienta de administración gráfica que simplifica la gestión del encaminador.

La posibilidad de filtrar paquetes mejora la seguridad y el rendimiento de la red. RRAS admite dos protocolos de encaminamiento:

- RIP (Routing Information Protocol), para IPX e IP.
- OSPF (Open Shortest Path First), solo para IP.

Lo más sobresaliente de esta actualización del RAS clásico son algunos parámetros que merecen ser mencionados porque ayudan a aumentar la seguridad en el uso del servicio RAS y son:

- **Require strong data encryption:** Esta opción, obliga a RRAS utilizar exclusivamente la codificación máxima de Microsoft (codificación de 128 bits), durante la comunicación; en esta opción, tanto servidor como clientes deberán configurarse para admitir el mismo nivel de codificación de datos.
- **Authentication Provider, Windows NT:** Esta opción proporciona servicios de autenticación a todos los clientes que realicen llamadas.
- **Authentication Provider, Radius:** Una opción que se permite si la red utiliza Remote Authentication Dial-In User Service (RADIUS) para autenticar a los clientes que realizan llamadas. Permitiendo utilizar un servidor RADIUS, de terceras empresas.

Además pueden ser usados los servicios de enrutamiento telefónico por petición para conectarnos remotamente de LAN a LAN a través de los vínculos WAN antes mencionados.

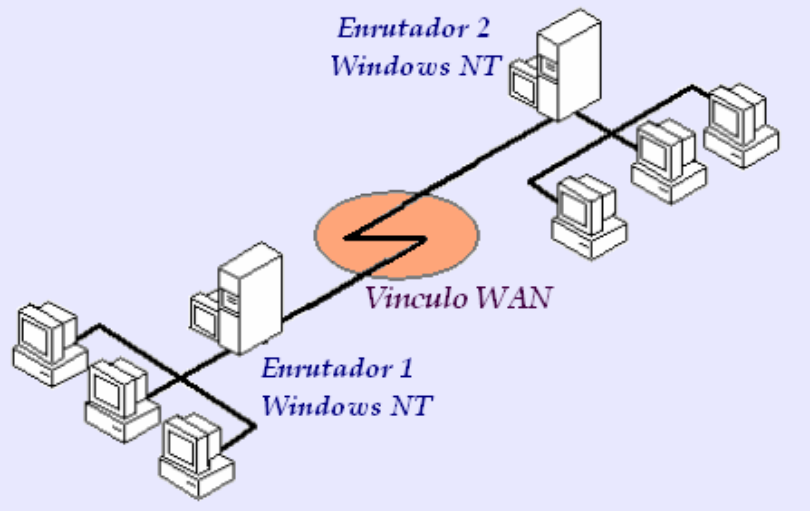


Figura 2.3: Escenario de enrutamiento de marcado a petición

2.5 Alternativas propuestas

Dentro de los servicios que se pueden activar ó implementar en una plataforma Windows NT Server 4.0, está el servicio de acceso remoto (RAS). Esta opción es una de las configuraciones que la institución podría realizar de forma rápida y lógica en términos de costo, para satisfacer sus necesidades de comunicación con el resto de oficinas ó clínicas remotas. Permitirá una conexión del tipo Punto - Punto ó Punto - LAN, en dependencia de lo que decida el departamento de TI de la institución.

La opción se tomó en cuenta porque este servicio corre bajo la plataforma actual, evitando variaciones en el entorno, disminuye los costos de la compra de una nueva plataforma, resulta más familiar para los administradores de la red ó del dominio, soporta las características del acceso remoto vía módem, a la cual se quiere adaptar la institución por su naturaleza de ONG (no esta en capacidad de pagar líneas de acceso dedicados guiados y permanentes, microondas o satelitales), y es de rápida configuración. Sin embargo, tiene ciertas desventajas de seguridad cuando se configura de manera inadecuada, que nos parecen de mucha importancia cuando se trata de mantener un buen nivel de acceso a toda la información privada del entorno informático. Esta alternativa tiene dos variantes, que se formularon teniendo en cuenta dos principales criterios muy importantes para implementar un servicio de este tipo. Los criterios son:

- Costo (primera alternativa NT).
- Seguridad y escalabilidad (segunda alternativa NT).

Cada una de estas variantes tiene dos entidades, el cliente y el servidor.

RAS por criterio **"Costo "**.

Identidad Servidor.

- Hardware y Software de conexión.
- Configuración del servicio.

Identidad Cliente.

- Hardware y Software de conexión.
- Configuración del Cliente RAS.

Nivel de Seguridad del servicio

2.5.1 Primera alternativa NT

Esta opción de configuración fue elaborada atendiendo al criterio "El costo" y no estrictamente ha razones técnicas. No necesitaremos ningún tipo de software extra para activar o implementar el Servidor de acceso remoto en el dominio, ni dispositivos dedicados para la seguridad. La configuración es **RAS** tradicional[6] sin ningunas variaciones más que las determinadas según los criterios de los administradores del dominio. Las variantes que el administrador puede hacer son personalizar los tipos de métodos de autenticación, propiedades del módem, protocolos LAN que podrán correr los usuarios remotos cuando se conecten a la LAN, activar las devoluciones de llamadas, etc. La plataforma WAN de conexión es la PSTN que tenemos en el país.

6 Activar solamente el componente de Acceso Remoto de Windows NT 4.0 y configurarlo.

2.5.1.1 Identidad Servidor

De acuerdo a una evaluación rápida del levantamiento de Hardware y software de la red, es recomendado utilizar el equipo UNISYS que esta actuando como un Member Server de la red, en otras palabras, un equipo Windows NT Server en configuración Stand - Alone. Su elección es justificada porque un equipo con esta configuración no participa de las solicitudes de Logon por parte de los usuarios del dominio, a diferencia de los equipos PDC y BDC de la red, de esta forma se entiende que tiene menos carga de trafico y menores tiempos de respuesta ante los nuevos usuarios remotos, además los servicios que actualmente proporciona no son de gran demanda y no generan una sobre carga de solicitudes de servicio. Esta elección es la más recomendada, sin embargo pueden utilizar otro equipo con Windows NT Server 4.0[7].

En la parte Servidor, proponemos activar él modulo de RAS que viene como parte de los servicios del sistema operativo de red, en este caso Windows NT Server 4.0. Además es importante haber instalado el Service Pack 6a y los últimos parches correspondientes a este servicio, para estar lo mas actualizado posible con las soluciones hechas al sistema e aplicaciones, puesto que estos resuelven muchos agujeros de seguridad[8]. El hardware que se necesita utilizar para esta variante es seleccionado de acuerdo a los recursos de hardware disponibles, y son los siguientes:

2.5.1.2 Hardware y Software Servidor

- Un equipo con sistema operativo Windows NT Server 4.0 y Service Pack 6a (puede ser el Member Server del dominio u otro equipo que cumpla con los requerimientos de Hardware del sistema operativo[9]).
- Tres módems externos (estos dispositivos ya los tiene la institución, especificación)
- Una tarjeta multipuertos serial de ocho puertos, marca EQUINOX (esta tarjeta debe comprarse, puede ver sus especificaciones en Anexos).
- Tres líneas telefónicas analógicas.

7 Un PDC, BDC ó un Member Server del dominio.

8 Consulte la dirección www.ntsecurity.net

9 Los requerimientos para instalar Windows NT Server 4.0, se pueden encontrar en los archivos reame.txt incluidos en el CD de instalación del sistema.

2.5.1.3 Configuración del Servicio

En esta sección mencionaremos los puntos a configurarse para instalar el servicio de acceso remoto, sin brindar una descripción detallada de los proceso de configuración del servicio. El primer paso para iniciar un RAS en Windows NT Server 4.0, es instalar el servicio, que puede ser instalado durante ó después de la instalación del sistema operativo. Al instalar el componente RAS se instalará también el acceso telefónico a redes que puede ser utilizado por el servidor RAS para conectarse con otros servidores RAS. Para iniciar y configurar RAS debemos hacerlo utilizando una cuenta de usuario miembro del grupo local de administradores. Una vez instalado el componente RAS, los puntos a configurarse son los siguientes:

- Instalar y configurar la tarjeta multipuertos serial y los módems externos. La configuración de la tarjeta multipuertos serial esta sujeta al software del fabricante.
- Seleccionar y configurar los protocolos que los clientes RAS podrán usar ó correr para tener acceso a los recursos del Servidor RAS y de la Intranet (si así lo permiten), especificar los métodos de autenticación y cifrado de datos.
- Crear cuentas de usuarios ó conceder permiso a cuentas ya creadas para permitir hacer conexión al servidor RAS.

2.5.1.4 Identidad Cliente

El equipo que actuará como cliente remoto, es cualquier equipo que tengan asignado para este propósito[10], que en términos de Hardware no demanda altas exigencias, más que las recomendadas por el sistema operativo y el servicio de acceso telefónico a redes.

2.5.1.5 Hardware y Software de conexión

- Un equipo con sistema operativo Windows 98 Segunda Edición.
- Un módem externo ó interno (compatible con los módems instalados en el servidor).
- Una línea telefónica analógica.

10 Ver en anexos, las características de los equipos remotos usados en las clínicas regionales.

2.5.1.6 Configuración del Cliente RAS

La configuración del cliente remoto, no exige de conocimientos especializados en acceso remoto, puesto que el sistema operativo tiene un ayudante de instalación lo bastante sencillo para entenderlo , sin embargo hay que tener el conocimiento para distinguir los parámetros que usará el módem para poder acoplarse con los módems que están instalados en la parte servidor(Marca del módem, puerto de comunicación, velocidades de transmisión, tipo de marcado, números telefónicos asignados, control de flujo y de errores, entre otros) . Esto es necesario para obtener una conexión confiable y estable. Los puntos de configuración son:

- Instale el módem a utilizar ó verifique que tiene uno ya instalado (externo ó interno).
- Ejecute el Acceso telefónico a redes (si lo tiene instalado), ó instálelo desde su ubicación correspondiente (Panel de control/Agregar ó Quitar programas/Instalación de Windows/comunicaciones/Acceso telefónico a redes) y luego lo ejecuta.
- Detecte el módem instalado y configúrelo según sus necesidades (por lo general los parámetros por defecto son los adecuados) e indique el número de teléfono al que llamará (Servidor RAS).
- Configure y verifique que las propiedades de la conexión son las requeridas para lograr una conexión libre de errores.

2.5.1.7 Nivel de Seguridad del servicio

El nivel de seguridad y acceso en esta alternativa del Servicio de Acceso Remoto, es muy discutida porque hay algunas vulnerabilidades en sus mecanismos de autenticación y cifrado (sino se actualizan con sus respectivos Service Pack y Parches), así como el uso de los sistemas operativos de los clientes remotos. Además la simplicidad del acceso remoto mediante los permisos que se le dan a la cuenta de usuario no permite aumentar las condiciones que el usuario necesitará reunir para aceptar una conexión al servidor RAS. Sin embargo las opciones de seguridad disponibles para esta alternativa son variadas, y una buena combinación de ellas puede dar como resultado un grado de seguridad aceptable

para entornos que no requieren seguridad extrema, pero nunca debemos pensar que es suficiente.

Construyamos y derrumbemos la seguridad

Aquí trataremos de describir los pro y contra de esta alternativa en función de la seguridad que nos puede ofrecer.

- El control del acceso a la red y sus recursos para los usuarios remotos, está basada en el método de control por contraseñas. **Pero es uno de los métodos más atacados hoy en día." Los usuarios son descuidados con sus contraseñas".**
- El sistema por si solo ofrece para este tipo de servicio el método de autenticación MS - CHAP y encriptación de datos sobre el vínculo como el mejor método de autenticación de usuario. **Si se usa respuesta de desafío, usando hash de LM es de poca ayuda el método de autenticación como el encriptamiento."Existe actualización a MS-CHAPv2 a clientes y servidores RAS solo conexiones VPN[11]"**
- Opción de retrollamada para asegurarse que la parte cliente reside desde una ubicación previamente conocida. **Las retrollamadas quitan movilidad al usuario; pero sino hay restricciones horarias de conexión, la línea se puede pinchar y utilizar." Si se tiene la clave de sesión es viable"**
- Con un simple permiso de llamada al Servidor RAS puedo intentar conectarme. **Se facilita al acceso no autorizado a presentar pocas condiciones para realizar la conexión.**
- Bloqueo de cuenta tras intentos fallidos[12] y concesión ó negación de permisos en la cuenta de usuario para ciertos recursos de la Intranet.

De los puntos mencionados anteriormente hay que destacar, la facilidad que tiene un usuario para conectarse a servidor RAS a cualquier hora del día, aunque podemos auditar su conexión, crea más poder de acceso a la red desde el exterior, cuando no definimos

11 Hay una actualización MS-CHAPV2 para clientes Windows98 y Windows98se, llamada DUN 1.4 en www.microsoft.com/windows98/downloads/corporate.asp

12 El bloque de cuentas debe ser limitante a 5 intentos por periodo de 30 minutos, según FC2 - E3 de ITSEC (Criterios de Evaluación de la Seguridad IT).

permisos restrictivos en el acceso a los recursos del NAS (Network Access Service) o a la Intranet. Como se puede notar en esta alternativa no existe una amplia cantidad de condiciones ó políticas de acceso remoto que restringa de forma particular, excluyente y estratégica el acceso del usuario remoto, no existe seguridad contra suplantación de identidad cuando se usan los protocolos de autenticación no actualizados (MS-CHAPv2[13]).No hay que olvidar que el servicio se compone de dos partes Cliente/Servidor, por lo tanto ambos deben estar al día con los Service Pack y parches, para que soporten los mismos protocolos de autenticación. Indudablemente se puede implementar el servicio RAS bajo las configuraciones que ofrece esta plataforma con este componente especifico(RAS), sin embargo la seguridad que se ofrece deja abierta algunas interrogantes ó posibilidades que pudieran darse, el sistema Windows NT Server como un componte limpio de sus actualizaciones conoce menos de las nuevas técnicas y herramientas para eludir sus fronteras.

2.5.2 Segunda alternativa NT

2.5.2.1 Descripción de la alternativa

RAS por criterio **"Seguridad y Escalabilidad"**

En esta sección de las alternativas, describiremos que otra opción se puede implantar con la plataforma actual. Con respecto a la opción anterior esta proporciona un mayor nivel de seguridad ante los accesos remotos externos a la Intranet y aumenta significativamente los alcances que puedan tener en el futuro las clínicas remotas (enrutamiento de LAN-to-LAN), en el caso de un aumento considerable de estaciones de trabajo ó implantaciones de subdominios. Esta opción retoma la mayoría de los requerimientos de hardware y software de la alternativa anterior, convirtiéndola viable desde el punto técnico, y la desarrollamos en el siguiente orden:

Identidad Servidor

- Hardware y Software de conexión.
- Configuración del servicio.

13 PPTP Performance update for Windows NT 4.0, evita las claves LANMAN y proporciona MS-CHAPv2, en la parte servidor.

Identidad Cliente

- Hardware y Software de conexión.
- Configuración del Cliente RAS.

Nivel de Seguridad del servicio

En esta alternativa pondremos en uso las actualizaciones que se han hecho al RAS tradicional de Windows NT Server 4.0, tratando de llevarlo a niveles más altos de control de los accesos de los usuarios remotos y dejando la implantación en una posición de escalabilidad. Además se requerirán más dispositivos de acceso telefónico (módems) en la parte servidor RAS, atendiendo a la condición de proporcionalidad que un pool de módems tiene para atender a usuarios (5 a 1), con la finalidad de brindar mayor nivel de disponibilidad a las solicitudes de conexión remota. La forma de aumentar la seguridad para un servidor RAS NT, es actualizándolo por el Servicio de Enrutamiento y Acceso Remoto (RRAS, es una actualización gratuita), que integra la posibilidad de utilizar un equipo intermedio entre el servidor RRAS (que ejecuta el RAS) y la Intranet, para agregar autenticación, autorización y auditoria, mediante el protocolo RADIUS. Con esta actualización RRAS podemos utilizar soluciones de terceras partes que nos ofrezcan sus versiones de servidores RADIUS. Sin embargo Microsoft ya cuenta con su propia versión de este protocolo, que lo encontramos en el Internet Authetication Services (IAS) del Windows NT 4.0 Option Pack y que no cuesta nada, para los que usuarios que han pagado por su licencia de Windows NT Server 4.0.

La alternativa consiste en instalar un servidor de enrutamiento y acceso remoto, que corra el servicio de acceso remoto y habilitarlo como cliente RADIUS, de un servidor RADIUS que corra el servicio de Autenticación de Internet (en esta caso el IAS de Microsoft), con el objetivo de aumentar las condiciones ó atributos que deben cumplir los usuarios remotos para obtener una conexión a la red o en un determinado equipo de la misma. Cada oportunidad que un usuario remoto intente realizar una conexión al servidor RAS, deberá presentar sus credenciales del dominio debidamente autorizadas y cumplir con condiciones previamente configuradas, como el tipo de servicio solicitado, tipo de puerto físico de acceso, regreso de llamada, protocolo de autenticación empleado, Id de cliente y tiempo de sesión entre otros; que hacen más seguro entregar un punto de conexión. Todas las credenciales de conexión del usuario remoto serán tomadas por el cliente RADIUS (Servidor RAS) y enviadas como un paquete Acceso-Solicitud de RADIUS al servidor RADIUS para su

correspondiente comprobación. El Servidor RADIUS no solo comprobara que el usuario remoto cumple con todas sus condiciones, sino también comprobara la identidad del cliente RADIUS que envía estas solicitudes apoyándose en una base de datos de usuarios del dominio, que en la mayoría de los casos y en este particular se encuentran en los controladores de dominio(PDC o BDC).

Cuando todas las credenciales y condiciones sean comprobadas con éxito por el Servidor RADIUS, este enviara todas los valores de configuración del usuario remoto al cliente RADIUS[14] para que este entregue el servicio solicitado, de esta manera esta alternativa se convierte en una estructura más robusta para autenticar y validar a los usuarios remotos dentro del dominio, cerrando las posibilidades de acceso no autorizado que se podrían suceder utilizando la primera alternativa de configuración del servicio de acceso remoto.

2.5.2.2 Identidad Servidor

Como mencionamos anteriormente, para esta alternativa seguiremos haciendo uso del equipo Member Server del dominio, como nuestro Servidor RAS (equipo UNISYS descrito en la alternativa primera alternativa NT), pero actualizando el componente RAS a RRAS (corriendo solo el servicio RAS) basados en las misma razones de su elección descritas en su correspondiente justificación, pero con la variante que a este servidor se le agregara un proveedor de autenticación RADIUS, que compruebe las credenciales de los usuarios remotos. El servidor RADIUS que proponemos instalar, podría correr en el BDC del dominio. La razón de proponer este equipo, es que posee una plataforma ya instalada (no necesitaremos comprar otra licencia de Windows NT 4.0 Server y evitamos hacer una inversión en otro equipo), además usaremos su base de datos de usuarios del dominio (SAM) para compartirla con el Servidor RADIUS local, así tendremos una base actualizada ante cualquier incremento en el numero de usuarios remotos dados de alta para este servicio, respuestas mas rápidas ante las solicitudes de comprobaciones de credenciales de usuarios y además este equipo tiene menos servicios que el PDC.

14 En la RFC 2138, puede encontrar ejemplos que muestran la forma de intercambio de paquetes de solicitudes y respuestas entre un cliente RADIUS y un servidor RADIUS.

2.5.2.3 Hardware y Software de conexión

- Dos equipos con sistema operativo Windows NT Server 4.0 y Service Pack 6a (que cumplan con los requerimientos de Hardware del sistema operativo).
- Archivo mpri386.exe (Para actualizar el componente RAS tradicional).
- El paquete software Windows NT 4.0 Option Pack (Para instalar el IAS).
- Cinco módems externos (estos dispositivos deben comprarse, detalle en Anexos)
- Una tarjeta multipuertos serial de ocho puertos, marca EQUINOX (esta tarjeta debe comprarse, puede ver sus especificaciones en (Anexos).
- Cinco líneas telefónicas analógicas.

2.5.2.4 Configuración del Servicio

Además de los puntos de configuración que describiremos mas adelante, debemos realizar ciertos cambios en el registro del servidor de acceso a la red (RRAS), ya que cuando se utiliza RADIUS como mecanismo de autenticación, no se puede ofrece MS - CHAPv1 a los usuarios remotos al momento de negociar el protocolo de autenticación, a menos que se realice un cambio en el registro del NAS[15]. Con el propósito de corregir algunos problemas que posee el IAS de Microsoft en su implementación de un servidor radius, es recomendado instalar el SP6a[16] y el Rollup Hotfix del IAS SP6[17].

La configuración del servicio en esta alternativa se divide en dos partes; la instalación y configuración de un servidor RADIUS a través del servicio de Autenticación de Internet(IAS de Microsoft) y la instalación y configuración de un servidor de acceso remoto a través del componente Enrutamiento y Servicio de Acceso remoto (RRAS de Microsoft).

Servidor RADIUS

- Instalar el sub - componente IAS del Internet connection Service para RAS que se encuentra en el Windows NT 4.0 Option Pack.

15 visite la dirección :www.microsfot.com y consulte el articulo 219283
16 visite la dirección :www.microsfot.com y consulte el articulo 241211, Lista de los errores que se corregibles con el Service Pack 6a.
17 Consulte el articulo 239864, http://download.microsoft.com/download/winntwebsvcs/nsp/1/NT45/EN-US/iassp6-x86.exe

- Configurar las propiedades del Servidor RADIUS, como son Service, logging, Cliente RADIUS y clave compartida, y los atributos de los usuarios habilitados para realizar Dial – Up al servidor RAS.

Servidor RAS

- Instalar y configurar la tarjeta multipuertos serial y los módems externos. La configuración de la tarjeta multipuertos serial esta sujeta al software del fabricante.
- Instalar archivo mpri386.ex, para actualización del componente RAS a RASS
- Seleccionar el componente a necesitar, en este caso RAS.
- Seleccionar los protocolos de red que los clientes RAS podrán usar ó correr para tener acceso a los recursos del Servidor RAS y de la Intranet (si así lo permiten), especificar proveedor de autenticación RADIUS y los protocolos de autenticación y cifrado de datos, así como métodos de direccionamiento.
- Reinstalar el Service Pack 6a.
- Crear cuentas de usuarios ó conceder permiso a cuentas ya creadas para permitir hacer conexión al servidor RAS.

2.5.2.5 Identidad Cliente

Los clientes que participan de esta alternativa, puede ser los equipos que actualmente existen en las diferentes clínicas remotas. Los sistemas operativos de estos equipos prestan los requerimientos mínimos para instalar el componente cliente remoto (acceso telefónico a redes), pero como esta alternativa descansa sobre una plataforma servidor Windows NT 4.0, pensamos que estos equipos deben ayudar a construir un entorno de conectividad remota segura y confiable, por tanto la seguridad local que ofrecen estos equipos debe ser coherente con nuestros objetivos de seguridad. Son muy conocidas las vulnerabilidades que presentan los sistemas Windows 95 y Windows 98 en los que respecta a saltarse inicios de autenticaciones a nivel de usuario y lo fácil que resulta instalar programas de cualquier tipo por cualquier usuario. Por tanto creemos que seria conveniente mantener equipos con sistemas Windows 2000 profesional, en lugar de los existentes, ya que este sistema resulta mejor en términos de accesibilidad y control local que los anteriores, aunque sabemos que

no están libres de un ataque de obtención de la cuenta del administrador del equipo local, sin embargo presenta menos vulnerabilidades conocidas y esta aun en continuo proceso de actualización a través del soporte que brinda Microsoft en sus Service Pack.

2.5.2.6 Hardware y Software de conexión

- Un equipo con sistema operativo Windows 2000 profesional (que cumpla con los requerimientos de hardware del sistema y tenga instalado Service Pack 4).
- Un módem externo o interno (compatible con los instalados en el servidor remoto).
- Una línea telefónica analógica.

2.5.2.7 Configuración del Cliente RAS

- Instale y configure el módem a utilizar ó verifique que tiene uno ya instalado (externo ó interno).
- Instale el componente acceso telefónico a redes e inicie el asistente para conexión de red, seleccione el tipo de conexión (Dial - Up) y el número o los números telefónicos de los servidores RAS.
- No permitir habilitar este componente para otros usuarios, y no habilitar el ISC (Internet Shared Connection), a menos que se requiera.
- Configurar las propiedades de la conexión (protocolos de autenticación, protocolos WAN y LAN).

Todas las opciones que se configuren en el cliente deben coincidir con los parámetros que espera recibir el servidor remoto para aceptar su petición de conexión.

2.5.2.8 Nivel de Seguridad del servicio

Sin lugar a dudas esta alternativa posee una estructura adecuada para la autenticación, autorización y auditoria de las conexiones mediante la aplicación de un protocolo estándar como lo es RADIUS, y deja muy por atrás la seguridad que proporciona la primera alternativa ofrecida con esta plataforma. Esta estructura es muy utilizada por ISP y

grandes empresas alrededor del mundo que ponen mucho interés en la seguridad de los accesos remotos a sus Intranet's y aunque este protocolo presente debilidades ante ciertos ataques como lo describe su RFC, la realidad es que nos permite tener una mayor fortaleza(cuando se utiliza información detallada de configuración para entregar un servicio al usuario) y flexibilidad en el control administrativo de los accesos remotos mediante una base de datos de usuarios centralizada en un entorno grafico y familiar al administrador del dominio. Además del uso de este estándar de seguridad RADIUS, incrementamos la seguridad en los sistemas operativos de los clientes a través de Windows 2000 profesional, a esto se le agregan las políticas de personal (quien controla las contraseñas, longitudes de contraseñas, periodos de cambios de contraseñas, penalizaciones a usuarios que presten sus contraseñas, pocos privilegios de administrador del equipo, entre otras). Es un sistema que trabaja sobre la estructura cliente/servidor ,por tanto el concepto de seguridad se aplica tanto desde el exterior como del interior porque los mensajes entre cliente y servidor Radius están encriptados, y tenemos la opción de elegir el protocolo de autenticación mas seguro que brinda NT 4.0 como es MS- CHAPv1 que nos permite el encriptamiento (sin lugar a dudas hubiéramos preferido MS- CHAPv2 pero no es aplicable en este entorno) para las conexiones externas, así como las condiciones que deben cumplir los usuarios remotos para permitirles el acceso a ciertos recursos , servicios o máquinas.

Capítulo III:

Propuesta de Conectividad RAS a través de Windows 2000 Server

Capítulo III: Propuesta De Conectividad Ras A Través De Windows 2000 Server

3.1 Servicios de Enrutamiento y Acceso Remoto

Para darnos una idea qué es y cuál es la función de este servicio, es necesario comprender un poco el concepto de enrutamiento, el cual tiene su complejidad y se describe en numerosos libros sobre redes. La comunicación entre hosts se realiza a través del intercambio de paquetes de red, los cuales se transportan por un medio de propagación que muchas veces puede tener cantidades de rutas hacia diferentes destinos, pero estos llegan a encaminarse en la ruta apropiada. El enrutamiento, es el proceso de usar la información de direccionamiento presente en un paquete de red, para determinar la ruta que debería tomar el paquete con el fin de alcanzar su destino; es necesario cuando el host de origen y el de destino se encuentran en redes lógicas diferentes.

Windows 2000 incluye un servicio de enrutamiento y acceso remoto, conocido mejor como **RRAS** (Router Remote Access Service), que se ha venido mejorando desde su primera distribución en 1996, este servicio RRAS reemplazó al servicio original **RAS** (Remote Access Service) de Windows NT Server 4.0. El RRAS de Windows 2000 trae nuevas características[18] que incluyen:

- Protocolo de administración de grupos de Internet (IGMP, Internet Group Management Protocol) y compatibilidad para los limites de multidifusión.
- Traducción de direcciones de red con componentes de direccionamiento y resolución de nombres (SOHO: Small Office / Home Office).
- Enrutamiento Apple Talk integrado.
- Compatibilidad de protocolo de túnel de nivel 2 (L2TP: Layer two Tunneling protocol) sobre seguridad IPsec con conexiones VPN de enrutador a enrutador.
- Herramientas de administración y control mejoradas. El programa de interfaz gráfica de usuario es la utilidad administrativa del RRAS, un complemento de la MMC (Microsoft Managment Console).

18 Estas características se agregan a las que ya tenia la versión RRAS de Windows NT 4.0

La fusión de los Servicios de enrutamiento y acceso remoto, ofrecen un nuevo producto que permite a un equipo donde se instala Windows 2000 Server funcione como:

- **Un enrutador multiprotocolo:** equipo que puede enrutar IP, IPX, APPLE TALK, simultáneamente.
- **Un enrutador de marcado a petición:** equipo que puede enrutar IP e IPX sobre vínculos WAN a petición o persistencia, ó sobre conexiones VPN.
- **Servidor de acceso remoto:** equipo que puede actuar como servidor de acceso remoto para proporcionar conectividad de acceso remoto a clientes de acceso telefónico ó de acceso remoto VPN, utilizando IP, IPX, Apple Talk ó NetBEUI.

La razón de integrar estos servicios de enrutamiento y acceso remoto como un solo servicio en la plataforma Windows 2000 Server , es para aprovechar la infraestructura que posee el protocolo PPP, en las negociaciones punto-a-punto de los clientes remotos, así como en las conexiones de enrutamiento de marcado a petición, ya que se encarga de negociar los parámetros de vínculos, intercambio de credenciales de autenticación de las partes que participan en el enlace y la negociación del protocolo de nivel de red.

3.2 Servicio de Acceso Remoto

El servicio de acceso remoto permite que clientes ubicados remotamente puedan conectarse a través de algún medio de transmisión a un servidor de acceso remoto. Tener acceso remoto permite que las aplicaciones se ejecuten en el cliente remoto y el control remoto lo que permite es compartir de forma virtual el equipo remoto, es decir, que todo lo que se ejecute con el control remoto se ejecuta en el host servidor de control remoto. La conectividad en este tipo de servicios que brinda Windows 2000, puede ser de dos tipos y están en dependencia de la infraestructura de transmisión por el cual se establece la conexión remota, estas son:

3.2.1 Acceso Remoto Telefónico

Ya sea de tecnología analógica o digital, permite el establecimiento de una conexión remota entre cliente y servidor, usando las condiciones que presentan las estructuras de

redes públicas y privadas que tienen como primer servicio básico el tráfico de voz **(PSTN, RDSI)** y datos **(X.25, ATM)**.

3.2.2 Red Privada Virtual (VPN)

La red privada virtual VPN, es una opción de conectividad que se caracteriza por usar la red pública mas grande del mundo (la World Wide Web, WWW), puesto que está soportada por el modelo TCP/IP.

3.2.3 Principales Elementos que forman una Conexión Remota de Acceso Telefónico

La comunicación es la acción de transmitir información a través de algún medio o canal de transmisión, desde una entidad denominada transmisora hacia otra denominada receptora. Este principio se mantiene en las comunicaciones de las redes de computadoras y en nuestro caso en las conexiones de acceso remoto, donde un sistema autónomo (cliente remoto) operado por una persona "X" envía datos a través de un medio de transmisión a otro sistema autónomo (servidor remoto) que decepciona, procesa y de ser necesario, reenvía dichos datos hacia otros sistemas autónomos para que sean convertidos en información útil para el usuario final (persona "Y"). Por tanto, para que pueda existir una conexión remota deben interconectarse los elementos de redes que interactúan en dicha comunicación, estamos hablando del cliente remoto, la infraestructura WAN (Wide Área Network) y el servidor remoto.

Cliente remoto: En Windows 2000 Server los clientes remotos soportados son: Windows NT 3.5 y posteriores (Microsoft) y los clientes no Microsoft que utilizan el protocolo de enlace PPP para acceder remotamente.

Servidor de acceso remoto: En este caso no hay duda que el receptor es un servidor Windows 2000 Server que tiene habilitado el servicio de enrutamiento y acceso remoto, que desde luego ha sido configurado para utilizar el servicio de acceso remoto.

Infraestructura WAN: La infraestructura WAN que se puede utilizar en este servicio de acceso depende de muchas variables y sobre todo de costos que se requieren para su implementación, por lo tanto la plataforma 2000 presenta alternativas que se pueden adaptar a las necesidades de comunicación y presupuesto proyectados. Las infraestructuras WAN que se toman en cuenta en esta plataforma son: **PSTN, RDSI, RED X.25 Y REDES ATM**.

3.3 Protocolos utilizados en el Acceso Remoto

3.3.1 Protocolos WAN

El acceso remoto de Windows 2000, soporta los siguientes protocolos de acceso remoto: PPP, SLIP y el protocolo RAS de Microsoft (conocido como NetBEUI asíncrono o AsyBEUI, es un protocolo de acceso remoto utilizado por los clientes de acceso remoto que utilizaban sistemas operativos antiguos como Windows NT 3.1, Windows trabajo en grupo, MS-DOS y LAN Manager). El acceso remoto de Windows 2000 es compatible con el Protocolo multi-vínculo (MP) PPP, el protocolo de asignación de ancho de banda (BAP) y el protocolo de asignación de control de banda (BACP). Estos protocolos se utilizan para formar un único enlace lógico a través de varios enlaces físicos y de esa manera crear enlaces de mayores anchos de bandas.

3.3.2 Protocolos LAN

Los protocolos de LAN que soporta Windows 2000 Server, son aquellos protocolos que pueden utilizar los clientes remotos para poder utilizar los recursos de la red remota. Los protocolos de acceso remoto que permiten hacer el enlace son como un puente que se establece entre dos computadores y por el cual pasarán los paquetes de los protocolos de red que son utilizados por los clientes remotos para poder hacer uso de los recursos disponibles dentro de la red y hacer peticiones a los computadores de la misma. Dentro de la red todos los computadores deben hablar un mismo idioma. Estos protocolos de red LAN son: TCP/IP, IPX, AppleTalk., NetBEUI.

3.4 Seguridad

3.4.1 Elementos que Brindan Seguridad en el Acceso Remoto

El sistema operativo de red Windows 2000, ofrece una amplia gama de características de seguridad, que incluyen:

- **Autenticación de usuario:** Proceso mediante el cual un sistema valida la información de inicio de sesión de un usuario, para asegurarse de su identidad.
- **Autenticación mutua:** Proceso en el cual los dos extremos de una conexión verifican la identidad del otro extremo.
- **Cifrado de datos:** Método usado para transformar u alterar la información mediante algoritmos, de tal manera que no pueda ser interpretada por quien no tiene el algoritmo de cifrado y su clave.
- **Devolución de llamada:** Mecanismo, que permite a un servidor remoto devolver la llamada de un usuario remoto después de haberle comprobado las credenciales de inicio de sesión, con el objetivo de ahorrar costo de llamada al cliente remoto y verificar su ubicación física.
- **identificador de llamada:** Opción de configuración que permite comprobar que una llamada entrante procede de un número telefónico determinado. Esta opción no devuelve la llamada, solo verifica el número del cliente remoto.
- **Bloqueo de Cuentas:** Característica de seguridad que se utiliza para bloquear una cuenta de usuario si se produce un determinado numero de intentos fallidos de inicio de sesión.
- **Directivas de acceso remoto:** Conjunto de condiciones y parámetros de conexión, que determinan si un intento de conexión específico se autoriza o se niega.

3.4.2 Elementos Básicos de la Administración de un Servicio de Acceso Remoto

Antes de proceder a implementar el servicio de acceso remoto se deben tomar en cuenta ciertos elementos que constituyen el éxito de dicha implementación, esto es:

- **Almacenamiento de cuentas de usuarios:** Espacio físico (equipo) donde residirá una base de datos que contenga las cuentas de los usuarios remotos. Con el propósito de tener una administración mas centralizada y segura.
- **Modo de asignación de direcciones y tipo:** La forma en que los clientes remotos obtendrán una dirección de red, ya sea de manera dinámica o estática y la clase de direccionamiento (pueden ser direccionamiento IP, IPX y AppleTalk).
- **Permisos de autorización del acceso:** Todas las opciones de configuración y condiciones de conexión que los clientes remotos deben cumplir para que se acepten sus solicitudes de conexión.
- **Proveedor de autenticación del acceso:** Son los servicios del dominio (Kerberos, RADIUS, NTLM), que comprueban las credenciales de los usuarios remotos que solicitan conexión.
- **Proveedor de cuentas de usuarios del acceso remoto:** Entidad autorizada, para proporcionar información de las cuentas de los usuarios (que componen su base de datos) a los servicios que comprueban las credenciales de los usuarios remotos.

De los elementos mencionados anteriormente depende la eficiencia de la administración del servicio y los clientes del mismo. Al iniciar el servicio RAS el administrador debe cumplir con el propósito que el servidor de acceso remoto envíe las credenciales de autenticación a un solo dispositivo de autenticación central. La asignación de direcciones es otro elemento de importancia al momento de identificar una maquina dentro de la red. El servidor de acceso remoto debe estar configurado para dar de alguna manera una dirección IP, dirección de red y nodos IPX, direcciones de redes y nodos AppleTalk, al momento que el cliente de ras lo solicite.

3.4.3 Proveedores de Autenticación

En Windows 2000 Server, los permisos para dar autorización de conexión a un usuario ya no será con la sencilla opción de conceder permiso de conexión de acceso telefónico, sino que dependerá de las propiedades de acceso telefónico de una cuenta de usuario y de las directivas de acceso remoto (Las directivas de acceso remoto son un conjunto de opciones de configuración y condiciones de conexión que proporcionan a los administradores de red

flexibilidad para autorizar los intentos de conexión). El servidor RAS de Windows 2000 tiene dos opciones que proporcionan un método de autenticación de los usuarios que soliciten una conexión remota:

- Los proveedores de autenticación que están son la autenticación Windows (autenticación Kerberos que en Windows 2000 esta por defecto, NTLM).
- Autenticación RADIUS.

La autenticación Windows:

- Hace que las credenciales de los usuarios remotos se autentiquen mediante los mecanismos normales de autenticación de Windows.
- Si el servidor de acceso remoto es un servidor miembro de un dominio de Windows nativo o mixto y se configura para realizar la autenticación mediante un proveedor Windows, entonces la cuenta del equipo servidor RAS deberá ser miembro de grupo de seguridad RAS e IAS.

Si la autenticación de los usuarios se realiza mediante un proveedor de autenticación RADIUS:

- Las credenciales y parámetros del usuario de la solicitud de conexión se enviaran como una serie de mensajes de solicitud RADIUS a un servidor RADIUS, para que este último decida si se acepta o deniega la solicitud de conexión.
- Un servidor RADIUS (un equipo que ejecute Windows 2000 Server y el servicio de Autenticación de Internet, conocido por las siglas IAS) recibe una solicitud de conexión de usuario del servidor de acceso remoto y autentica al cliente en su base de datos de autenticación.
- Además, un servidor RADIUS puede agregar otros parámetros de conexión que hacen más restringido el uso de la conexión permitida (Tiempos máximos de sesión, asignación de direcciones IP estáticas, etc).

Un servidor RAS:

- Puede configurarse para que utilice Windows ó RADIUS como proveedor de cuentas.
- Si se selecciona Windows, entonces la información de las cuentas se guardan en un archivo de registro en el servidor RAS. Si se utiliza RADIUS, entonces se envían los mensajes de cuentas RADIUS al servidor RADIUS para que se guarden y se analicen posteriormente. El proveedor de las cuentas es el que mantiene las cuentas de los usuarios de acceso remoto.

Cuando se tienen un conjunto de servidores de acceso remoto ó servidores VPN Windows 2000 Server en múltiples localizaciones geográficas y se desea que todos los servidores utilicen un conjunto centralizado de directivas de acceso retomo para autorizar las conexiones entrantes, entonces debe configurarse un equipo que ejecute Windows 2000 Server y el servicio de Autenticación de Internet (IAS) y luego configurar cada servidor de acceso remoto ó VPN como un cliente RADIUS para el equipo servidor IAS. Esto mantiene un mayor control administrativo sobre los servidores RAS.

3.4.4 Directivas de Acceso Remoto

Las conexiones de acceso remoto se aceptan en base a las propiedades de acceso remoto telefónico de una cuenta de usuario y de las directivas de acceso remoto. Una directiva de acceso remoto es un conjunto de condiciones y parámetros de conexión que determinan las características de la conexión entrante, así como el conjunto de restricciones que se le imponen. Las directivas de Acceso Remoto se pueden utilizar:

- Para especificar las conexiones permitidas y condicionadas por factores como: la hora del día y el día de la semana, el grupo de Windows 2000 al que pertenece el usuario de acceso telefónico, el tipo de cliente de acceso remoto (telefónico o VPN) y otras condiciones.
- Para imponer parámetros de conexión tales como: máximo de tiempo que una conexión puede tener un cliente RAS, métodos de autenticación segura necesarios,

cifrado necesario, herramientas de control y administración de los clientes de acceso remoto, así como su control y la solución de problemas de conexión.

Con múltiples directivas de acceso remoto se pueden aplicar diferentes conjuntos de condiciones a acceso remoto diferentes, o bien se pueden aplicar diferentes requisitos al mismo cliente de acceso remoto basándose en los parámetros del intento de la conexión. Con la utilización de una mezcla de directivas de acceso remoto se puede realizar lo siguiente:

- Permitir ó denegar conexiones si la cuenta de usuario pertenece a un grupo especifico.
- Determinar días y horas diferentes para las diferentes cuentas de usuario, en función de la pertenencia a grupos.
- Configurar diferentes métodos de autenticación para los clientes de acceso remoto telefónico y VPN.
- Configurar diferentes opciones de autenticación y cifrado para las conexiones del protocolo de túnel punto a punto (PPTP) ó protocolo de túnel de capa 2 (L2TP).
- Configurar diferentes tiempos de máximos de sesión para las diversas cuentas de usuario, en función de la pertenencia a grupos.
- Enviar atributos RADIUS específicos del servidor de acceso de red a un cliente RADIUS.

Las directivas de acceso remoto son una parte medular del control de los intentos de conexión en Windows 2000 Server junto con los permisos conocidos en las versiones anteriores de los servidores RAS de NT. En la figura 3.1 se muestra el papel regulatorio que tiene una directiva en el procesamiento de un intento de conexión remota. La figura describe como se procesa el intento de conexión remota de un usuario con credenciales validas dentro del dominio, cuando se utilizan las propiedades de Dial –Up de su cuenta de y las directivas de acceso remoto.

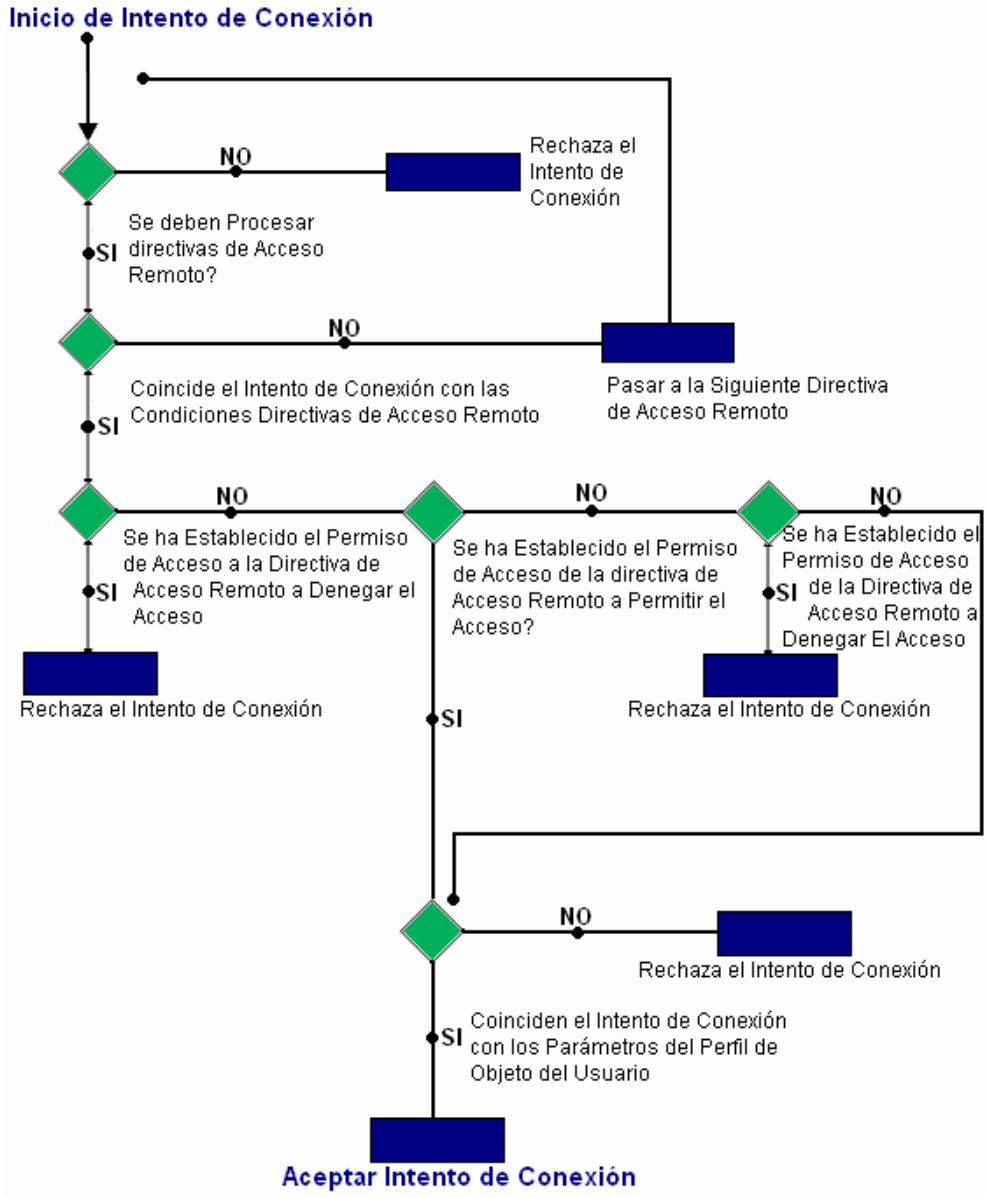


Figura 3.1: Uso de Directivas al Momento del Intento de Conexión

3.5 Propuesta de Alternativa Windows 2000

Esta opción que presentamos es una visión de la implementación que la institución puede alcanzar cuando halla llegado al punto de actualización de la plataforma que actualmente opera, que lógicamente es su siguiente punto evolutivo de su entorno Windows y es conciente que la plataforma actual se puede volver un poco insegura a medida que pasa el tiempo ya que el soporte que proporcionaba Microsoft se ha retirado (Service Pack, Parches, etc.).

No es una alternativa que pueda darse de manera acelerada y desordenada, puesto que hablamos de grandes costos económicos y funcionales (operaciones administrativas) que pudieran presentarse sino se ejecuta de acuerdo a un plan metodológico de actualización de plataforma. En este apartado no podríamos hablar de implementar un Servicio de Acceso Remoto basado en Windows 2000 Server, dentro de un entorno Windows NT 4.0 sin hablar de la migración[19] ó la actualización. Sin embargo ese tema abarca una complejidad que va más allá de probar las ventajas que brinda un solo servicio, de nuestros conocimientos y experiencia que hemos acumulado durante la elaboración de este trabajo monográfico.

Migrar implica una tarea que requiere un dominio de las características del sistema actual y del sistema futuro, para realizar una valoración de las ventajas que este ultimo pueda tener para nuestros propósitos u objetivos. Tiene que darse bajo un proceso de planificación muy bien elaborado donde se aborden las estrategias que el departamento de TI tomara antes de actualizar su dominio, se debe conocer al detalle la estructura de los nombres de dominio de la institución para darse cuenta si es necesario una reestructuración de ellos y aprovechar los beneficios de la nueva estructura administrativa que proporciona la nueva plataforma, todos los tipos de hardware y software que componen la estructura del dominio para detectar donde existen puntos estratégicos y ordenar una secuencia de actualización , que sistemas operativos y equipos están listos para actualizarse, compatibilidades de las versiones de software, estrategias de recuperación de los sistemas, intervalo de tiempo en pasar de **Modo Mixto** (Es la configuración predeterminada de Windows 2000, el modo mixto permite a los controladores de dominio de Windows 2000 y a los controladores de reserva de los dominios Windows NT coexistir en un mismo dominio) **a Modo Nativo** (La condición en la cual todos los controladores de dominio de un dominio son controladores de dominio Windows 2000 y un administrador a activado la operación en modo nativo), las implicaciones de ello sobre la seguridad del entorno y muchas otras actividades.

En conclusión hablar de actualización y lo que de ella derivan para un entorno cualquiera ó en este caso PROFAMILIA, es un tema que merece un desarrollo muy técnico y

19 Leer capitulo 10, del libro titulado "Windows 2000 Server Guía de implantación "que se encuentra en la sección de bibliografía o visite la Web http://www.microsoft.com/latam/windows/server/implementacion.htm

profesional. Por consiguiente nuestra alternativa Windows 2000 se aplica asumiendo que la fase de evaluación de migración fue hecha sin ningún problema y el equipo en que se correrá el servicio de enrutamiento y acceso remoto ya fue actualizado a Windows 2000 Server con todos los servicios que prestaba anteriormente ó con los que estimen convenientemente los administradores del Dominio.

Además, recomendamos que el primer equipo en ser actualizado sea el PDC, para aprovechar al máximo las características[20] que ofrece Windows 2000 Server cuando esta en modo mixto. Esta es la opción más acertada porque en términos de costos y funcionalidad, es absurdo y de poco provecho actualizar como primer paso el equipo que trabaja como Member Server, solo por el hecho de utilizar el servicio de enrutamiento y acceso remoto en un dominio Windows NT 4.0.El costo beneficio de tener un plataforma Windows 2000 Server corriendo como Member Server y con servicios como RRAS y otros que se pudiesen agregar, no es coincidente para un dominio con las proporción y características que posee esta institución(en términos de administración y ventajas que ofrece este nuevo sistema operativo de red), un Member Server no proporciona las características del Directorio Activo[21]. Los servidores miembros pertenecen a un dominio, pero no contienen una copia de los datos del Directorio Activo.

La alternativa esta expuesta de la siguiente manera:

Identidad Servidor

- Hardware y Software de conexión.
- Configuración del servicio RAS.

Identidad Cliente

- Hardware y Software de conexión.
- Configuración del Cliente RAS.

Nivel de Seguridad del servicio

20 Ver tabla de Disponibilidad de las características de Windows 2000 Server en modo mixto.

21 El Directorio Activo es un servicio de directorio de Microsoft Windows 2000 que reemplaza al administrador de cuentas de Windows NT 4.0. El Directorio Activo consta de un bosque, uno o mas dominios, unidades organizativas, contenedores y objetos, en el se pueden representar varias clases de objetos, como usuarios, grupos, equipos y aplicaciones.

3.5.1 Identidad Servidor

3.5.1.1 Hardware y Software Servidor

- Un equipo con sistema operativo Windows 2000 Server y Service Pack 4 (que cumpla con requerimientos óptimos de Hardware del sistema, operando en modo mixto).
- Cinco módems externos (nuevos, especificación)
- Una tarjeta multipuertos serial de ocho puertos, marca EQUINOX (esta tarjeta debe comprarse, puede ver sus especificaciones en Anexos).
- Cinco líneas telefónicas analógicas.

3.5.1.2 Configuración del Servicio RAS

Como mencionamos anteriormente la configuración del RAS esta regida por la siguiente condición:

- El equipo debe ser un PDC (Windows NT Server 4.0) actualizado a Windows 2000 Server (es un controlador de dominio emulando[22] un PDC) y trabajando en modo mixto, ya que suponemos que por alcance de costos solo se ha comprado una licencia para un solo servidor y el resto de los equipos servidores del dominio son Windows NT Server 4.0.

El proceso de instalación de un servidor RAS a través del servicio de RRAS que ofrece Windows 2000 Server, no es muy diferente de su versión anterior, sin embargos si lo es en aspectos de contener mas opciones de seguridad, pero por ahora solo mencionaremos los puntos de configuración que debemos ejecutar para activar nuestros servicio de acceso remoto y permitir a los usuarios acceder a la Intranet y sus recursos.

Siempre es preferible que instalemos este servicio con una cuenta de administrador del dominio para que se realicen de forma automática ciertos procesos como la adición del

22 Los controladores de dominio contienen copias exactas de las cuentas de usuario y otros datos de Active Directory de un dominio dado. Un equipo Windows 2000 que emula a un PDC, actúa como un controlador de dominio principal de Windows NT, en el sentido que realiza las tareas de un controlador PDC, incluyendo la replicación de los datos del dominio en todos los controladores de reserva del dominio.

servidor RRAS al grupo de seguridad de servidores RAS e IAS cuando es un servidor miembro, en nuestro caso la cuenta del equipo será parte de este grupo. Los puntos a configurar son los siguientes:

- Instalar y configurar la tarjeta multipuertos serial y los módems externos. La configuración de la tarjeta multipuertos serial esta sujeta al software del fabricante.
- Ejecutar Wizar: Windows 2000 Configure Your Server y activar el servicio de RRAS.
- Elegir de las cinco opciones que permite la configuración del RRAS, el servicio que necesitamos (RAS).
- Seleccionar los límites de acceso que tendrán los usuarios de acceso remoto y los protocolos LAN que podrán utilizar, modo de asignamiento de direcciones IP, modo de administración (Windows o RADIUS).
- Eliminar la directiva de acceso remoto que esta por defecto y crear nuevas directivas de acceso remoto que se adapten a nuestros propósitos y niveles de seguridad requeridos (configurando las Condiciones, permiso de acceso remoto y perfil).
- Configurar las propiedades del servidor RAS.
- Conceder los permisos de acceso remoto en las cuentas de los usuarios o crear las cuentas de usuarios y darle los permisos de acceso remoto (solo están activados Permitir (acceso, Denegar acceso, y devoluciones de llamada).
- Configurar las auditorias de las conexiones remotas (opcional).

3.5.2 Identidad Cliente

3.5.2.1 Hardware y Software de conexión

- Un equipo con sistema operativo Windows 2000 profesional con Service Pack 4.
- Un módem externo ó interno (compatible con los módems instalados en el servidor).
- Una línea telefónica analógica.

3.5.2.2 Configuración del Cliente RAS

- Instale y configure el módem a utilizar ó verifique que tiene uno ya instalado (externo ó interno).

- Instale el componente acceso telefónico a redes e inicie el asistente para conexión de red, seleccione el tipo de conexión (Dial - Up) y el número o los números telefónicos de los servidores RAS.
- No permitir habilitar este componente para otros usuarios, y no habilitar el ISC (Internet Shared Connection), a menos que se requiera.
- Configurar las propiedades de la conexión (protocolos de autenticación, protocolos WAN y LAN).

Todas las opciones que se configuren en el cliente deben coincidir con los parámetros que espera recibir el servidor remoto para aceptar su petición de conexión.

3.5.3 Nivel de Seguridad del servicio

Indudablemente los niveles de seguridad que brinda un servidor de enrutamiento y acceso remoto Windows 2000 Server, son mayores que los encontrados en la versión de Windows NT Server 4.0 y mencionar cuales son estas mejoras en el RAS solo seria volver a mencionar el apartado "**Elementos que brindan Seguridad en el Acceso Remoto"** que describimos en paginas anteriores. Sin embargo hay un detalle que nos parece de sumo cuidado y peligrosidad dentro de esta configuración cuando proponemos activar el RRAS en el equipo que emula al PDC del dominio para utilizar las ventajas de administración y seguridad que nos brinda Windows 2000 Server y es el hecho que permitimos conexiones remotas a un servidor clave en el cual descansan servicios sensibles y las cuentas del dominio.

Para este caso, en donde los riesgos de un acceso no autorizado y con suficientes derechos de administración podrían ser destructivos, es necesario alcanzar niveles de seguridad muy altos, sin entrar en la compra de equipos dedicados a este servicio y que estamos seguros que pueden fácilmente desarrollarse mediante la infraestructura de directivas de seguridad que permite esta plataforma y con ayuda de políticas de personal.

En conclusión esta alternativa pueda darse sin ningún problema, y debemos recordar que los clientes deben ser Windows 2000 profesional para crear una mejor coherencia entre sistema cliente/servidor (un entorno Directorio Activo), la seguridad puede ser confiable si:

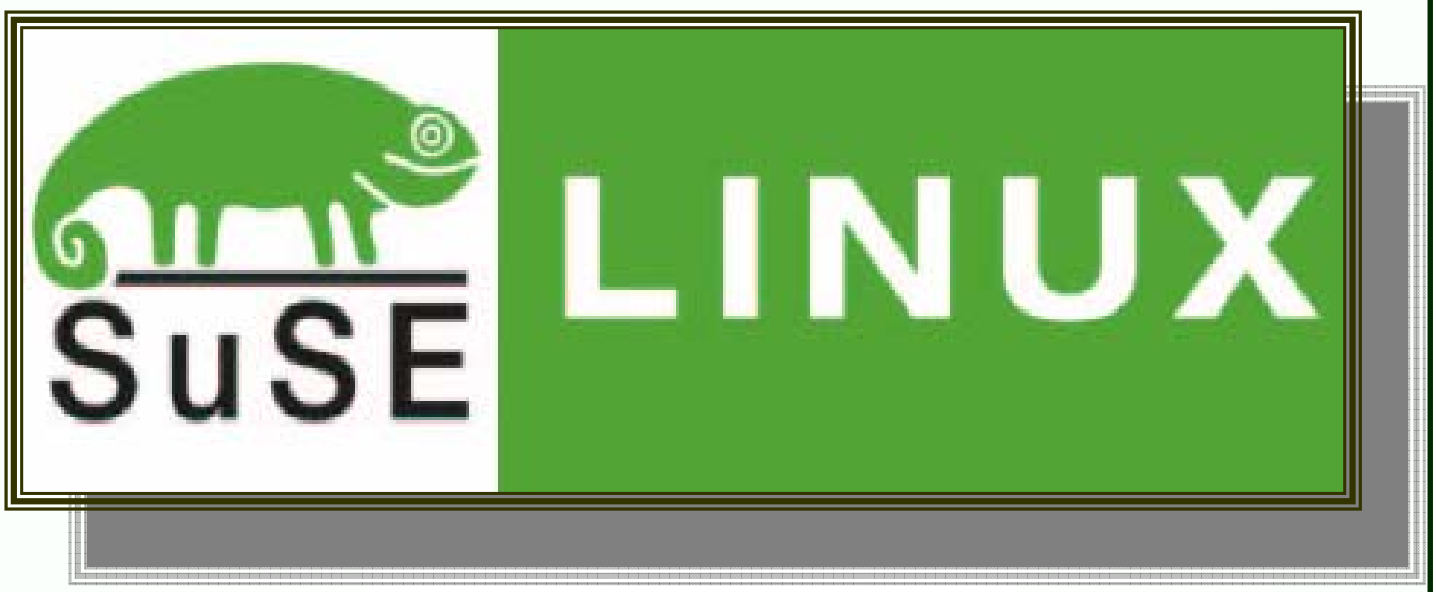
Aplicamos un buena política al acceso de las maquinas remotas, permitiendo las conexiones a ciertos usuarios, y el uso de contraseñas robustas y de cierto mínimo de tamaño (contraseñas de administración del equipo, del perfil del usuario y de la sesión de conexión remota), así como un cambio periódico de estas ultimas.

Restringimos la distribución de los números de teléfonos de nuestro servidor RRAS.

Aplicamos adecuadas directivas de acceso remoto, y el protocolo de autenticación mas seguro, la encriptación de los datos, métodos de direccionamiento de direcciones de red, filtrado de paquetes de ser necesario (como método de firewall[23]), y las opciones del perfil de la cuenta de usuarios que ayuden con la seguridad. Sin olvidar el bloqueo de cuentas de acceso remoto. Administrar a los usuarios remotos por grupos y aplicarles directivas de seguridad dentro del dominio para restringirle permisos a los dispositivos, servicios y directorios que estén solamente relacionados con su trabajo.

Aplicar auditorias y seguimientos de los sucesos que estas registren, sobre las conexiones de acceso remoto. Se debe recordar que con el servidor RRAS, se ofrece la escalabilidad en el momento en que se necesiten conexiones de LAN a LAN.

23 Filtración de paquetes: Trabajan a nivel de red y los paquetes son filtrados en función de su tipo, su dirección de origen, su dirección de destino y la información de acceso en el paquete. Se consume poca CPU y disminuye el tiempo de espera en la red porque analizan poca información. El problema se encuentra en si se utiliza DHCP (asignación dinámica de direcciones IP) ya que la única manera de identificación del usuario es la dirección IP que se ha asignado a su puesto de trabajo.



Capítulo IV:

Propuesta de Conectividad Ras A Través de Suse Linux 8.0

Capítulo IV: Propuesta De Conectividad Ras A Través De Suse Linux 8.0

4.1 Acceso Remoto y Servidor PPP

4.1 VPN y PPP

La redes Virtuales Privadas (VPN), permite a las estaciones remotas conectarse a la red privada de forma segura a través de redes Públicas y normalmente usa la Internet como enlaces seguros comunicando oficinas aisladas lo que decrece los costos ya que el acceso es generalmente local y la información es transportada por un túnel establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte, lo que permite el acceso remoto a servicios de red de forma transparente y segura. Estas utilizan PPP[24] para crear un túnel de forma dinámica de punto a otro para transferir datos a esto se le conoce como encapsulación además los paquetes son encriptados por PPP de forma que los datos que viajan a través del mismo sean ilegibles para los extraños, asegurando la privacidad de la conexión entre ambos ordenadores. Como lo muestra la siguiente Figura:

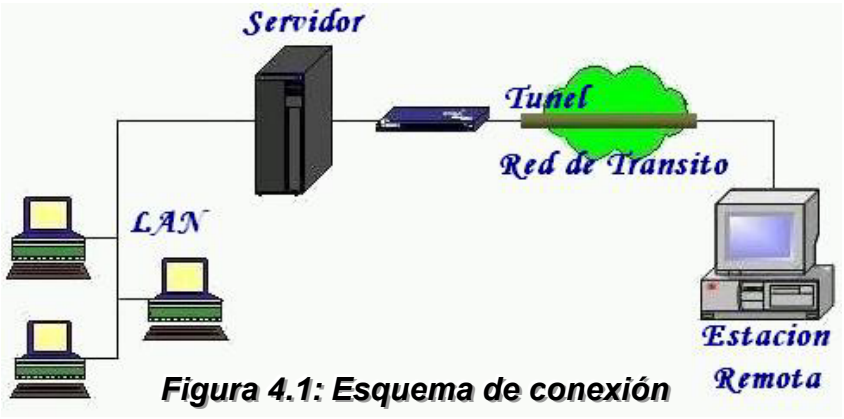


Figura 4.1: Esquema de conexión

Dos protocolos que se pueden utilizar para realizar la conexión remota son: PPP y SLIP[25], aunque este ultimo es menos completo. Además PPP admite transportar paquetes de distintos protocolos como IP, IPX, Alpanet y permite tener todos los protocolos y servicios de TCP/IP a través de una línea telefónica, definido en RFC 1661, fue diseñado para transportar

24 Point to Point Protocol (PPP): Es un protocolo que permite establecer una conexión analógica sobre un puerto serie bajo el Protocolo de Internet (IP) – (Guía de Administración de Redes II- Suse Linux).

25 Diseñado Para conectar estaciones de trabajo bajo Sun a través de Modém (Redes computadoras, Pág.229, A. Tanenbaum – Pearson -3ª Edición)

paquetes entre identidades homólogas, que proporcionan operaciones bidireccionales simultáneas asumiendo la entrega de paquetes de forma ordenada y proporciona un método para el transporte de datagramas, teniendo tres componentes principales:

- **Un método para encapsular datagramas del multi-protocolo.**
- **Link Control Protocol para establecer, configurar y probando la conexión del Data-Link.**
- **Network Control Protocols para establecer y configurar los protocolos de capa de red.**

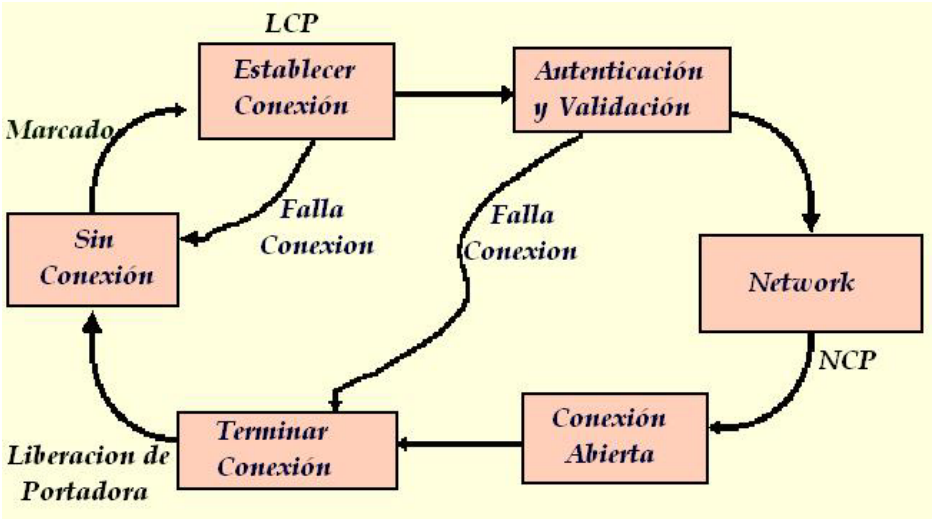


Figura 4.2: Funcionamiento de PPP

4.1.2 Servidor PPP

Este servidor es capaz de validar y rechazar la solicitud de conexión del usuario remoto. El daemon pppd asume el control una vez establecida la conexión y actualiza las configuraciones de red; al establecer la conexión se generará una nueva ruta con nuevas direcciones IP asignadas dinámicamente y se actualizará el fichero que contiene información sobre los servidores de nombres, luego se encarga del registro o autenticación de usuario mediante el uso de PAP[26]/CHAP[27], proceso durante el cual intercambian información relativa a la identificación de usuario, de forma que ambos exijan una correcta autenticación. Una vez que se ha realizado el proceso de registro, no hay ninguna diferencia entre servidor y cliente. Un aspecto importante radica en la velocidad del medio de transmisión a utilizar que en

26 Password Authentification Protocol (PAP): Proporciona un método simple para establecer identidad utilizando negociación de dos vías. (Guía Completa de Protocolos de Telecomunicaciones, Pág. 329 – McGraw Hill - 1ª edición).

27 Challenge Handshake Authentification Protocol (CHAP): Verifica las identidades periódicamente utilizando negociación de 3 vías. (Guía Completa de Protocolos de Telecomunicaciones, Pág. 317 – McGraw Hill - 1ª edición).

nuestro caso es la Línea Telefónica, que oscila entre 56 kbps y 33,6 kbps dependiendo de las especificaciones del módem, estas velocidades pueden variar dependiendo de las horas picos en las transmisiones telefónicas. Antes de establecer una conexión PPP en el servidor, hay que disponer de la siguiente información:

- **El número de teléfono del ordenador al que se va a llamar.**
- **El tipo de dirección IP asignada.**
- **La dirección IP del servidor DNS del proveedor.**
- **Datos necesarios para realizar la autentificación.**

4.1.3 Servicio de Acceso Remoto (RAS)

Un equipo con RAS permite a otro conectarse a él mediante una línea telefónica y un módem con ayuda de PPP, este se encarga de establecer la comunicación entre las máquinas remotas y es capaz de detectar errores, permitir la negociación de IP y verificar la autentificación de los usuarios al momento de la conexión. Una vez conectado la estación remota trabaja se integra físicamente a la red y acceder al host utilizando servicios basados en TCP/IP como Telnet o FTP. Además es posible configurar uno o varios módems RDSI en un mismo servidor para que actúe como un Servidor de Acceso Remoto con conexiones telefónicas conmutadas. Este Servicio incluye:

- **Configuración del servidor PPP para la recepción de conexiones.**
- **Configuración del esquema de autenticación PAP y/o CHAP.**
- **Configuración de un cliente de acceso remoto.**

El costo del servicio es gratuito, únicamente se paga el tiempo que permanece conectado, a costo de llamada local. Para realizar una conexión Ras se necesita:

- **Un servidor RAS**
- **Una línea telefónica y un módem**
- **Software de conexión a Internet, Como:**
  - **Protocolos de acceso a la red, autorización y automatización**
  - **Programas de explotación de Internet: navegadores, correo, etc.**

4.1.4 Protocolos de Comunicación entre Servidores

4.1.4.1 Network Information Service (NIS) (Interfaz Linux – Windows)

Base de Datos distribuidas que sirve para proveer información a través de la Red como: Nombres de login, passwords, directorios e información de grupos. Además es un sistema de autentificación dentro de una red mediante el cual una vez validada una contraseña en uno de los computadores que formen parte de la red, no tiene que validarse la entrada a los recursos que conforman el sistema NIS. Los dominios NIS tienen una función administrativa y son transparentes a los usuarios. NIS esta basado en RPC[28] e incorpora a un servidor, una biblioteca con las funciones del lado del cliente y varias herramientas de administración. En una red debe tener al menos un servidor NIS, aunque se pueden tener múltiples servidores, cada uno sirviendo a diferentes dominios NIS, donde uno es el llamado servidor NIS maestro, y todos los demás son los llamados servidores NIS esclavos. Las bases de datos NIS están en el formato DBM, que deriva de las bases de datos ASCII. El servidor NIS maestro debe tener ambas, las bases de datos ASCII y las DBM. Los servidores esclavos serán notificados de cualquier cambio en los mapas NIS, y recibirán automáticamente los cambios necesarios para sincronizar sus bases de datos. Los clientes NIS no necesitan hacer esto ya que estos siempre hablan directamente con el servidor NIS para leer la información almacenada en sus bases de datos. El mapeador RPC es un servidor que convierte números de programas RPC en números de puerto de protocolo TCP/IP o UDP/IP. Debe ejecutarse para poder realizar llamadas RPC a servidores RPC de esa máquina. Cuando un servidor RPC arranca, avisa al mapeador por cuál puerto está escuchando y a que números de programas RPC está preparado para servir, cuando un cliente desea hacer una llamada RPC a un número de programa dado, primero debería contactar con el mapeador de puertos del servidor, para determinar el número de puerto al que los paquetes RPC deben ser enviados. Normalmente el mapeador de puertos debe ser iniciado antes los servidores RPC. Cada vez que los usuarios cambien sus passwords, la base de datos NIS y probablemente otras bases de datos que dependan de la base de datos NIS de los passwords deben ser actualizadas.

28 RPC (Remote Procedure Call): Protocolo de llamada a procedimiento remoto que especifica el formato de la comunicación entre el cliente y el servidor. El cliente envía sus peticiones RPC al servidor, este procesa y devuelve los resultados en una respuesta RPC(Linux Guía de Instalación y administración – V. López – McGraw Hill – 1ª edición)

4.1.4.2 Network File System (NFS)

Sistema de ficheros en la red que permite que varios nodos de una red puedan acceder a ficheros remotos como si los tuvieran en su propio disco local. La información de propiedad de los ficheros que un servidor NFS proporciona a sus clientes viene dada por los valores numéricos de identificador del usuario y de grupo. Por lo tanto, esto resulta útil si el cliente y el servidor tienen el mismo mapa de usuarios y de grupo que se obtiene en los nodos de un servidor NIS. Hay dos implementaciones posibles de NFS en Linux:

- **Servidor en el Espacio de Usuario:** Usa las llamadas RPC del espacio de usuarios, permite exportar del servidor NFS la jerarquía de los directorios del espacio usuarios, viendo estos la misma jerarquía de directorios vista en el servidor, además es fácil hacer mapeo, DNS, NIS, NIS+, etc.
- **Servidor en el Espacio del Núcleo:** se prefiere este servidor por consideraciones de rendimiento e Inter-operación.

4.4.1.3 Services for UNIX (Interfaz Windows – Linux)

Es un paquete adicional para Windows utilizado para entornos mixtos, que posibilita la co-existencia de Windows y UNIX, además incluye una amplia gama de utilidades que permiten migrar fácilmente aplicaciones desde UNIX a Windows. Mejor dicho, usando protocolos estándar y los distintos servicios de SFU, le permite a los clientes con entorno UNIX trabajar sobre plataforma Windows utilizando sus aplicaciones y scripts en lenguaje nativo UNIX y hacerlos compatibles con las aplicaciones Windows. Service for Unix se divide en tres partes: Servidor NFS, Cliente NFS y la entrada NFS. Con la copia de los archivos compartido en otros servidores permite la rápida recuperación de los puntos caídos, además usa sus Protocolos para autenticar a los usuarios del dominio y los recursos para ser compartidos. Un servidor NIS utiliza un programa residente para la sincronización de contraseñas y un intérprete de mandatos y utilidades utilizadas en la línea de mandatos de UNIX. La sincronización de contraseñas con el Servidor NIS mejorar la seguridad de la red apoyote en el uso encriptación de contraseñas, usa NIS para autenticar archivo sistema acceso y llevar a cabo la sincronización de la contraseña en las plataformas que no tienen

SFU, las bibliotecas del encriptación son incluido con el código de la fuente, simplificando recopilación y aplicación. Network File System (NFS) ofrece una significativa mejora en el rendimiento, permitiendo a los usuarios acceder a archivos de forma sencilla en máquinas que funcionan tanto bajo Windows como bajo UNIX. Además, a través de una sincronización de contraseñas de doble vía mejorada, nombre de usuario y NIS, las empresas pueden integrar o centralizar los servicios de directorio a través de las plataformas UNIX y Windows. Por lo tanto, la gestión del directorio se convierte en un proceso mucho más fácil y que requiere menos recursos. Además, las capacidades de registro dinámico que permitirán a los administradores de redes hacer cambios como ajustar el rendimiento de la red, sin que el sistema tenga lapsos de caída, que antes sólo se resolvían reiniciando la máquina. Utilizando el servidor Telnet compatible permite iniciar sesiones autentificadas y la nueva emulación cliente y servidor NFS, La aplicación Telnet que se incluye en SFU dispone de una importante característica que es la captura de sesión.

4.2 Correo Electrónico

4.2.1 Protocolos

***SMTP* (*Simple Mail Transfer Protocol*):** Regular el envío de correos electrónicos en Internet de forma uniforme y está definido en **RFC 821**; desde sus orígenes ha experimentado innumerables ampliaciones y se caracteriza por los siguientes rasgos distintivos:

- **Establece conexión directa entre origen/destino o los procesos implicados.**
- **La función es la transmisión del mensaje y no la recepción o almacenamiento.**
- **El cliente y el servidor se comunican por medio de comandos legibles.**
- **Todos los mensajes serán confirmados o pueden ser reenviados.**

Los comandos SMTP posibilitan una comunicación directa entre el remitente y el destinatario, desarrollo típico de un proceso de protocolo de una sesión **Telnet en el puerto 25**[29] del servidor de correo. En la figura se representa este proceso:

29 Puerto estándar para servidores de correo en Internet (Redes de Computadoras, Pág.658 – A. Tanenbaum, Editorial Pearson, 3ª edición).

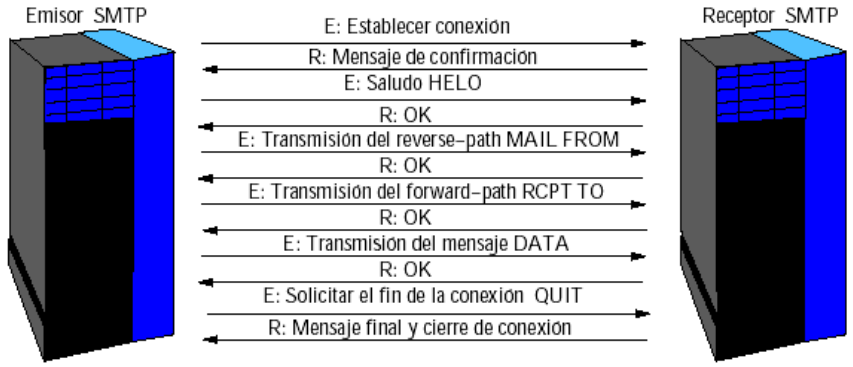


Figura 4.3: Desarrollo del Tráfico SMTP[1]

- **MTA (*Message Transfer Agent*):** Designa procesos capaces de transmitir correos de A hacia B, esta es la función del SMTP en el lenguaje especializado, estos son:

  - **Sendmail**
  - **Postfix**
  - **Qmail**
  - **smail.**

- **MUA (*Mail User Agent*):** Se aplica cuando actúa como interfaz entre usuario y mensajes, designa una herramienta para recibir, procesar y enviar correos, entre ellos:

  - **Mutt**
  - **Pine**
  - **Mail**
  - **GNUs**
  - **Kmail**
  - **N. Messenger**
  - **MS Outlook.**

- **MDA (*Mail Delivery Agent*):** Designa proceso que se ocupan de la entrega local en el buzón del usuario, que funciona entre el MTA y el MUA, entre ellos:

  - **Deliver**
  - **Procmail**

Después de determinar que el destinatario de un correo recibido se encuentra en el sistema local, el servidor SMTP (MTA) inicia localmente el MDA y le entrega dicho correo, este se ocupa de depositarlo y agregarlo a un buzón. A partir de este momento el usuario puede procesar el mensaje localmente mediante POP3.

POP3[30] **(*Post Office Protocol Versión* 3):** Permite acceder dinámicamente al almacén de correos del Host servidor, definido en la **RFC 1939**

El inconveniente de poseer tan sólo una interfaz es mitigado por sus características, como fiabilidad, estabilidad, eficaz manejo y la posibilidad de ejecutarlo en ordenadores remotos mediante telnet, rlogin y ssh. Los servidores de correo electrónico intentan verificar otro servidor basándose en una consulta de nombres DNS y/o una consulta DNS inversa, el conjunto de reglas define el tratamiento de las direcciones incompletas que aparezcan en la cabecera de un correo. Existen casos de múltiples buzones de usuarios que se distingue por las siguientes características:

- **POP3 regula la transmisión de un mensaje cuando ésta es iniciada**
- **El cliente establece conexión basada en TCP en el puerto 110 del servidor**
- **El cliente y el servidor intercambian comandos hasta que la conexión finalice**
- **Los comandos se transmiten en texto abierto, al igual que los argumentos**
- **El servidor transmite un mensaje sobre la situación de la comunicación**
- **Exige una autentificación del cliente ante el servidor**
- **Se da una fase de transacciones donde se transmiten uno o varios correos**
- **Cuando se cierra la conexión, el servidor entra en una fase de actualización**

4.2.2 Servidor de correo

Sendmail[31]**:** Es complejo en cuanto a su administración y funciona a través del socket 25 comunicándose para recibir y enviar correo, utiliza SMTP el cual se caracteriza por su eficiencia, sencillez y facilidad de depuración, procesando mensajes en prácticamente cualquier tipo de red; emplea un gran archivo de configuración que hace referencia a archivos de configuración, sintaxis extraña y extensión considerable, al punto de que existe un sistema de generación del archivo con miras a evitar la manipulación directa del mismo. Un servidor de correo sólo acepta mensajes que van dirigidos al dominio en que está dado de alta. Sendmail abre una conexión contra el mail server remoto, este

30 Post Office Protocol V.3 (POP3): Permite acceder al almacén de correos en un host servidor (Redes computadoras, Pág.662, A. Tanenbaum – Pearson -3ª Edición

31 Sendmail: delivery que proporciona servicio de email en Linux, conocido como. (Pág.96 - Administración de Redes II- Suse Linux)

envía su nombre de máquina local, nombre del emisor, buzón de destino y un comando diciendo que empieza el texto del mensaje. El servidor finaliza el tratamiento y comienza a aceptar el mensaje hasta que recibe una marca especial, ambos programas entienden que el envío de comandos ha sido retomado. La llamada a mail sin argumentos permitirá a un usuario leer el correo que se encuentre almacenado en su buzón de correo que presenta los mensajes perfectamente ordenados, con objeto de poder ser accesibles de manera independiente.

4.3 Seguridad en Red

4.3.1 Principio de Seguridad

Consiste en mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin y mantener bajo protección los recursos y la información con que se cuenta en la red a través de procedimientos basados en una política[32] de seguridad que permitan el control. La complejidad de la implementación de estas medidas requiere de un alto compromiso organizacional, agudeza técnica y constancia para renovar y actualizar dicha política en función de la organización. Las políticas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto por administrar sus recursos y reconocer factores que facilitan la normalización y materialización de los compromisos de la organización. De aquí dos conceptos básicos de seguridad que son:

- ***Seguridad Local:*** **Consiste en diferenciar a unos usuarios de otros, de modo que ningún pueda obtener derechos de otro.**
- ***La seguridad en la Red:*** **Consiste en proteger el sistema entero contra ataques provenientes de la red.**

32 Las políticas son el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad del sistema, esto constituye las alarmas y compromisos compartidos de la organización ya que le permiten actuar pro-activamente ante situaciones que comprometan su integridad. (Manual de Administración – Suse Linux).

4.3.2 Security Shell[33]

Ofrece una autenticación completa (Login, password) y comunicación codificada, SSH de Suse Linux ofrece un alto nivel de seguridad debido a la complejidad del sistema de seguridad, con la implementación del sistema se obtienen alternativas a telnet, rlogin, rsh y rcp, donde los datos que transmiten pueden ser fácilmente interceptadas por elementos externos, este sistema soporta la protección de conexiones X11 y TCP al reenviarlas por un canal seguro criptográficamente es caracterizado por la baja velocidad de transmisión, ocasionada por la difícil técnica de codificación. Sus funciones son:

- Registro Remoto
- Ejecución interactiva o no interactiva de comandos remotamente
- Copiar ficheros entre ordenadores
- Autentificación y comunicación segura criptográficamente sobre redes inseguras
- Sustituye herramientas rlogin, rsh y rcp
- Reenvío de puertos (port forwarding)
- Sistema de túneles (tunneling)

Características especiales de SSH:

- Validación del servidor a través de algoritmos criptográficos RSA[34]
- Control de usuarios a través de ficheros de configuración a todo el sistema
- Transmisión y compresión de datos binarios entre ordenadores
- El cliente dispone de seis métodos distintos para validarse de cara al servidor
- Codificación automática y transparente de la comunicación

También ofrece al usuario la oportunidad de realizar una conexión encriptada con una computadora remota, los filtros de paquetes posibilitan un control adecuado sobre el tráfico de datos en la red, los paquetes de filtrado permiten que una computadora ejerza de enrutador para unir una red interna a una única dirección IP visible desde afuera a través de

33 Security Shell (SSH): Es una aplicación multiplataforma ideada para permitir una comunicación segura sobre la administración de sistemas Remotos (Linux Guía de Instalación y administración – V. López – McGraw Hill – 1ª edición)

34 Referida a la clave de acceso remoto al servidor (Linux Guía de Instalación y administración – V. López – McGraw Hill – 1ª edición)

masquerading (Adaptación NAT[35]), donde un enrutador tiene más de una interfaz de red que se conecta con el exterior. La dirección de destino de respuesta es el enrutador, que debe reconocer el paquete y modificar la dirección de destino para que aterrice en la computadora correcta, este reconocimiento de paquetes ocurre con ayuda de una tabla que se mantiene directamente en el kernel del enrutador, mientras las conexiones estén activas.

Una conexión ya establecida tiene un estado asignado en las tablas, de tal forma que esta entrada no pueda ser utilizada por una segunda conexión. Existen distintos tipos de firewall[36] que de hecho se diferencian en el nivel lógico y abstracto en el que se examina y controla el tráfico de datos. Un filtro de paquetes regula el pasaje siguiendo criterios como el protocolo, el puerto y la dirección IP e intercepta paquetes que no deberían entrar en su red, dos configuraciones básicas son:

- ***Personal-firewall:*** **Diseñado para abrir Internet en conexiones que no requieran configuración, mantenimiento y no permiten el paso de ningún paquete.**
- ***SuSEfirewall2:*** **Configuración más Segura.**

Es posible conectar un sistema a distancia y trabajar de forma interactiva, sustituyendo a telnet y rlogin, donde el enlace simbólico adicional de nombre apunta igualmente a SSH. Después de haber conseguido una autentificación válida se podrá trabajar ya sea con la línea de comando o de forma interactiva, además ofrece también la posibilidad de transferir de forma recursiva todo un directorio. Al iniciarse por primera vez genera tres pares de llaves que se componen de una parte pública y una privada. Para garantizar la comunicación segura, únicamente el administrador debe tener el derecho de acceder a las claves privadas, las partes públicas de las llaves se traspasan a todos los partners en comunicación.

El cliente que pide una conexión, intercambia datos de identificación con el daemon, utiliza los mismos protocolos para evitar la conexión a puerto equivocado. Al utilizar SSH se procede a mandar su clave pública host key y un server key que crea el daemon cada hora,

35 Network Address Translation: Traducción de Direcciones de Red (Administración de Redes I- Suse Linux)

36 Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la red privada e Internet (The Oficial Red Hat Linux Reference Guide - Red Hat Linux 8.0)

por medio de estas claves el cliente encripta una clave que varía cada sesión e indica al servidor el tipo de encriptado. Para desencriptar la clave es imprescindible disponer de las claves privadas de host y server; estas no se pueden obtener a base de las partes públicas, por eso únicamente daemon es capaz de descifrar la clave mediante su clave privada. SSH puede realizar la autenticación mediante otro juego de llaves creados a petición, donde el programa indica donde se guardan la clave privada y la pública. La parte pública de la clave se ha de copiar a la computadora remota.

SSH facilita el trabajo con aplicaciones de X-Windows remotas, al utilizar la variable DISPLAY en la estación remota que se configura automáticamente y todas las ventanas del X-Windows se mandan a través de la conexión SSH existente a la computadora cliente, esto evita las posibilidades de captura de datos por parte de terceros en caso de aplicaciones X-remotas con visualización local.

4.3.3 Autenticación de Red y Kerberos

Aparte de los mecanismos habituales de identificación que son inherentemente inseguros, no existe ninguna forma de autenticar exactamente en una red abierta, donde cualquier persona puede ser capaz de falsificar su identidad y así recoger los correos de otra persona, acceder a los datos privados de ella o iniciar un determinado servicio. Por eso la red debe cumplir los siguientes requisitos para poder ser considerada como segura:

- ***Los usuarios deben acreditar su identidad para cada servicio y se debe asegurar que ningún usuario acoja la identidad de otro.***

- ***Cada servidor en la red debe acreditar su identidad, para evitar que un atacante puede identificarse como el servidor solicitado y capturar la información confidencial que se esté mandando a éste. Este proceso se llama "Mutual Authentication", ya que el cliente se identifica frente al servidor y viceversa.***

La autentificación Kerberos[37] es del tipo ***Trusted Third Party*** en el que todos los clientes le confían respecto a la identidad de otras computadoras. Kerberos mantiene una base de datos con todos los usuarios y sus claves privadas, para que merezca la confianza depositada en él, el servidor de autenticación y el servidor que otorga los tickets han de ejecutarse en una máquina aparte. Sólo el administrador debe tener acceso al servidor y los servicios a ejecutar deben reducirse al mínimo, ni siquiera sshd debe estar levantado. Al introducir la contraseña, la información del nombre del sistema de otorgamiento de tickets, se envía al servidor Kerberos, si reconoce la identidad, genera una clave de sesión al azar para el uso entre el cliente y el servidor de otorgamiento. El servidor de autenticación genera un ticket para el servidor de otorgamiento de tickets que se compone de:

- ***Los nombres de los clientes y del servidor de otorgamiento de tickets***
- ***La hora actual y El tiempo de vida del ticket.***
- ***La dirección IP del cliente y La clave de sesión nueva***

El ticket se envía junto a la clave de sesión de forma encriptada, utilizando la clave privada del cliente, solo el cliente y Kerberos conocen esta clave, cuando el cliente recibe esta información, tiene que introducir la contraseña, entonces esta se convierte en la clave capaz de descifrar la información enviada del servidor de autenticación. Luego la contraseña y la clave se borran de la computadora; es capaz de identificarse correctamente hasta que el tiempo de vida del ticket otorgado expire. Para pedir un servicio de cualquier servidor en la red, la aplicación del cliente tiene que compulsar su identidad, por eso la aplicación genera un identificador que se compone de las siguientes partes: ***El Principal del cliente, El IP del cliente y la hora actual.*** El servidor utiliza su copia de la clave para decodificar el identificador, que le permite obtener toda la información necesaria del cliente, que es comparada con el ticket. Es posible realizar la autenticación en ambas direcciones, para evitar cualquier tipo de ataque, aquí tanto el servidor como el cliente se solicitaran la apropiada autenticación. Kerberos implementa un mecanismo para obtener tickets de los diferentes servidores que se denomina servicio de otorgamiento de ticket (Ticket Granting Service). Siempre que una aplicación necesita un ticket que aún no se haya otorgado,

37 Kerberos original se desarrolló en el MIT, con el fin de los clientes no enviaran las claves sin cifrar. Aparte de éste existen otras implementaciones. SuSE Linux contiene una implementación libre de llamada Heimdal Kerberos 5 KTH, por lo que siempre se utiliza el término Kerberos salvo que se trate de propiedades específicas de Heimdal (Manual de Administración – Suse Linux).

contacta el servidor de otorgamiento. La solicitud de un ticket se compone de las siguientes partes:

- ***El Principal solicitado***
- ***El ticket para el otorgamiento de ticket y El identificador (authenticator)***

El servidor de otorgamiento controla el recibo e identificador, en caso de confirmar la autenticidad, genera una clave de sesión nueva que se debe utilizar para la conexión y se da la creación de un ticket para el servidor nuevo con la información siguiente:

- ***El Principal del cliente y del servidor***
- ***IP del cliente y La hora actual***
- ***La clave de sesión recién creada.***

El ticket se envía junto a una clave de sesión al cliente, con respuesta encriptada, ahora el cliente es capaz de descifrar la respuesta de un servicio nuevo que se solicite sin necesidad de pedir la contraseña de usuario. No hace falta introducir ninguna contraseña para utilizar estas utilidades.

Criptografía: Esta resuelve problemas de seguridad de privacidad que se logra si se cifra el mensaje, integridad de la información, autenticación referida a la confirmación de la persona y del mensaje y el no rechazo referido a la no negación de la autoría del mensaje enviado, se divide en dos grandes ramas:

- **Criptografía Simétrica:** son un conjunto de métodos que permiten la comunicación segura, cuando hayan intercambiado la clave correspondiente (clave simétrica), conocida criptografía de llave privada, clasificada en tres familias: criptografía simétrica de bloques, criptografía simétrica de lluvia y criptografía simétrica de resumen. Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas.
- **Criptografía Asimétrica:** Utiliza dos claves diferentes, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada, sus principales

aplicaciones son el intercambio de claves privadas y la firma digital38. Dividida en tres familias la primera basada en Problemas de factorización, la segunda basada en Problemas del Logaritmo Discreto (PLD), y la tercera basada en Problemas del Logaritmo Discreto Elíptico. Existen otros sistemas que se basan en problemas del Logaritmo Discreto Hiperelíptico, problemas de retículas y subconjuntos de clases de campos numéricos reales y complejos.

4.3.4 Políticas de Seguridad

Es importante establecer políticas de seguridad en un sistema informático debido a los constantes ataque de virus u otras personas. La planificación de las políticas de seguridad se divide en seis etapas diferentes:

- **Planificación de las necesidades de seguridad:** Existen diferentes clases de seguridad, por lo que, dependiendo del tipo de sistema, habrá que dar mayor o menor importancia a las que tengan más relevancia:

  - **Confidencialidad:** Impedir el acceso a la información a usuarios no autorizados.
  - **Integridad de los datos:** Evitar el borrado o alteración indeseados de la información, incluidos los programas.
  - **Disponibilidad:** Asegurar que los servicios esté siempre disponibles para un usuario autorizado.
  - **Consistencia:** Asegurar que el sistema se comporta como esperan los usuarios autorizados; imagine lo que ocurriría si el comando *ls* borrara archivos de vez en cuando en lugar de listarlos.
  - **Control:** Reglamentar el acceso al sistema, de forma que programas e individuos no autorizados y desconocidos no alteren el normal funcionamiento del sistema.
  - **Auditoria:** Determinar qué se hizo, quién lo hizo y qué fue afectado. Para esto es necesario llevar un registro inexpugnable de todas las actividades realizadas

38 Firma Digital es una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario.

en el sistema y que identifica de forma no ambigua a los usuarios que las llevaron a cabo.

- **Análisis de riesgos:** Trata de responder a tres preguntas: ¿qué se debe proteger?, ¿contra qué debe protegieres?, ¿cuánto se está dispuesto a invertir para obtener una protección adecuada? Para responder a estas preguntas, el análisis de riesgos se divide en tres etapas:

  - **Identificación de los activos**
  - **Identificación de las amenazas**
  - **Cálculo de los riesgos**

- **Análisis de costo-beneficio:** Consiste en asignar un costo a cada riesgo, y determinar el costo de defenderse. De esta manera se puede decidir qué medidas hay que adoptar para proteger qué activos. Este aspecto no lo desarrollaremos por que no entra en el ámbito de este estudio.

- **Políticas de seguridad:** Las políticas sirven para definir qué se considera valioso y especifican qué medidas hay que tomar para proteger esos activos. Deben aclarar qué se está protegiendo, establecer la responsabilidad de la protección y poner las bases para resolver e interpretar conflictos posteriores. No deben hacer una lista de riesgos específicos, computadoras o individuos por nombre. Deben ser generales y no variar mucho a lo largo del tiempo.

- **Implementación**

- **Auditoria y Respuesta Ante Incidentes:** Estos dos últimos apartados constituyen el resto de este trabajo.

4.3.5 Niveles de seguridad

Los requisitos para un determinado por un nivel de confianza pudiendo restringir más los criterios, de seguridad, esta jerarquía de niveles esta detallada a continuación del menor al mayor:

- **Seguridad Mínima:** En esta categoría están englobados todos los sistemas que han sido valorados y no han superado los requisitos mínimos para pertenecer a un nivel de seguridad superior. En esta categoría no existen requisitos de seguridad. "En realidad ningún sistema pertenece a esta categoría, puesto que ningún vendedor evaluaría un sistema para obtener un nivel de seguridad "D". Ordenadores bajo MS-DOS o las versiones personales de Windows (familia 9x), además de otros sistemas antiguos son un ejemplo de sistemas que pertenecerían a esta categoría.

- **Protección Mediante Seguridad Discrecional:** Todos los usuarios manejan los datos al mismo nivel. En este nivel se procura evitar que los usuarios cometan errores y dañen al sistema. Las características más importantes de este nivel son el control de autentificación mediante contraseñas y la protección discrecional de los objetos. El código del sistema debe estar protegido frente a ataques procedentes de programas de usuario (en UNIX, un proceso no puede salirse de su espacio virtual de direcciones, y si lo intenta, morirá. Un sistema de este nivel no necesita distinguir entre usuarios individuales, Tan solo entre tipos de accesos permitidos o rechazados. En UNIX C1 hay que ser dueño de un objeto para ceder sus derechos de accesos y siempre se protege a los objetos de nueva creación.

- **Protección Mediante Accesos Controlados:** A partir de este nivel, el sistema debe ser capaz de distinguir entre los usuarios individuales. Generalmente el usuario debe ser dueño de un objeto para ceder los derechos de acceso sobre él. En la mayoría de los sistemas UNIX a partir de este nivel, existen listas de control de acceso (ACLs). Debe permitir que los recursos del sistema se protejan mediante accesos controlados. En UNIX el acceso a los periféricos (dispositivos de E/S) siguen un esquema de permisos idéntico al de los ficheros de los usuarios. Se aplican los requisitos de reutilización de objetos cuando esos mismos se reasignan.

Se requiere a partir de este nivel que el sistema disponga de auditoria. Por ello cada usuario debe tener un identificador único que se utiliza para comprobar todas las acciones solicitadas. Se deben auditar todos los sucesos relacionados con la seguridad y proteger la información de la auditoria. El sistema debe ser capaz de auditar a nivel de usuario. La mayor parte de los UNIX comerciales pertenecen a este nivel, puesto que lo único que han tenido que añadir los fabricantes es un paquete de auditoria.

- **Protección Mediante Seguridad Etiquetada:** A partir de este nivel, los sistemas poseen un sistema de control de accesos obligatorio que implica colocar una etiqueta a los objetos (principalmente sobre los ficheros). Esto, junto con el nivel de habilitación de los usuarios es utilizado para reforzar la política de seguridad del sistema. En estos sistemas, el dueño no es el responsable de la protección del objeto, a menos que disponga de la habilitación necesaria. En cuanto a la auditoria, el sistema debe ser capaz de registrar cualquier cambio o anulación en los niveles de seguridad, y también hacerlo selectivamente por nivel de seguridad." Debe existir una documentación que incluya el modelo de seguridad soportado por el sistema. No es necesaria una demostración matemática, pero si una exposición de las reglas implantadas por las características de seguridad del sistema.

- **Protección Estructurada:** A partir de este nivel, los cambios en los requisitos no son visibles desde el punto de vista del usuario respecto de los niveles anteriores. En B2, todos los objetos del sistema están etiquetados, incluidos los dispositivos. Deben existir vías fiables que garanticen la comunicación segura entre un usuario y el sistema. Los sistemas deben ser modulares y utilizar componentes físicos para aislar las funciones relacionadas con la seguridad de las demás. Requieren una declaración formal del modelo de seguridad del sistema, y que haya una gestión de la configuración. También deben buscarse los canales ocultos.

- **Dominios de Seguridad:** Es necesario que exista un administrador de seguridad, que sea alertado automáticamente si se detecta una violación inminente de la seguridad. Deben existir procedimientos para garantizar que la seguridad se

mantiene aunque el ordenador se caiga y luego arranque. Es obligatoria la existencia de un monitor de referencia sencillo, a prueba de agresiones e imposible de eludir. La TCB debe excluir todo el código fuente que no sea necesario para proteger el sistema.

- **Diseño Verificado:** Esta es la clase de certificación más alta, aunque el Libro Naranja no descarta la posibilidad de exigir requisitos adicionales. Son sistemas funcionalmente equivalentes a B4. Tan solo se añade la distribución fiable que refuerza la seguridad. Los sistemas A1 tienen la confiabilidad adicional que ofrece el análisis formal y la demostración matemática de que el diseño del sistema cumple el modelo de seguridad y sus especificaciones de diseño.

4.4 Propuesta de Alternativa

4.4.1 Implementación a Nivel de Software

El servicio de acceso remoto (RAS), es uno de los servicios que se puede activar en un servidor con Suse Linux, es una opción rápida de configurar y de costos bajos por las ventajas que trae el sistema y que a criterio nuestro puede satisfacer las necesidades de comunicación que tiene PROFAMILIA. Se toma en cuenta a Suse Linux por las ventajas que podemos encontrar en este sistema frente a otros sistemas operativos como son: Precio, Seguridad, Estabilidad, Crecimiento, etc. Factores que pueden ser de gran provecho para el desempeño de la institución, por lo que se propone la instalación de un servidor de RAS con Suse Linux 8.0 para realizar las comunicaciones de las clínicas departamentales con la Oficina central y que trabaje en conjunto con el servidor de Windows NT 4.0 que es el que provee a la Oficina central el Internet y el servicio de mensajería. Con una buena configuración y administración de Suse Linux se alcanzarán los mejores niveles de comunicación y seguridad. Esto se propone realizar organizadamente, recomendando la debida capacitación del administrador para el eficiente uso del nuevo sistema.

4.4.2 Implementación a Nivel de Hardware

Linux como SOR es una herramienta muy poderoso, por lo que el migrar todos los servicios de Windows NT 4.0 a Suse Linux 8.0, tendría sus complicaciones principalmente al momento de trasladar la base de datos que se tiene bajo SQL – Server, ya que podría presentar incompatibilidades con MySQL de Linux. Este servidor RAS tendrá un vínculo con servidor Compaq (servidornt), en el que esta configurado los servicios que brinda IFX, para brindarle todos que necesitan las clínicas departamentales. Para minimizar tiempo y costos de la implementación, se activarán los servicios Acceso Remoto, Correo, seguridad y autenticación y un acceso a los servidores de base de datos que existen actualmente, proponiendo realizar la migración de los servicios restantes poco a poco, cuando la institución lo crea conveniente, hasta alcanzar la completa migración de todos los servicios a Linux.

Debido a la cantidad de clínicas que tiene la institución, se realizará la conexión RAS con ayuda de una tarjeta adaptador multipuertos[39] de 8 puertos de los cuales se usaran 5 puertos y 3 puertos quedaran para futuras integraciones de estaciones a la red (Clínicas Regionales) y se escogerá de acuerdo a criterios técnico y soporte del fabricante en Linux. Este a su vez estará conectada a 5 Módems (que también se escogerán de acuerdo a las especificaciones del fabricante) cada uno conectado a una línea de la red pública o PSTN (una vez que aumenten la cantidad de líneas de 3 a 5), ya que la institución no está en capacidad de pagar líneas de acceso dedicados u otro medio de transmisión que aunque mejoraría la eficiencia y velocidad en la transferencia de archivos, también elevarían los costos operativos de la misma.

La mayoría del hardware que se utilizará está en el inventario de la institución y serán reutilizados, lo que lleva a una adquisición mínima de nuevos hardware lo que deja un ahorro considerable. La configuración se realizara de la siguiente manera:

39 Características del adaptador multipuesto SST – Puertos Universal PCI Adapter (3.3v -5v). hoja de datos – Apéndice B

Figura 4.4: Esquema de Conexión con RAS

La plataforma WAN de conexión es la red telefónica Nacional o PSTN que tenemos en el país. Existen tres líneas telefónicas que se van a usar para la conexión, junto a un Adaptador Multipuertos (que se debe comprar) con soporte en Suse Linux, además de 5 Módems Externos (que se deben comprar), ya que son 20 Clínicas con las que la institución mantiene comunicación en todo el país (incluyendo la futura unión de Bluefields a la red de comunicación de PROFAMILIA, ya que es la única clínica sin conexión) y debido a la proporción de 4 estaciones por cada Módem, además se necesitará comprar dos cuñas telefónicas para satisfacer este requerimiento. El esquema de trabajo que se seguiría es:

Cada una de las Línea telefónica tendrá asignado un grupo de estaciones Remotas como se muestra en la Figura 4.4, estas asignación de estaciones se hará por su ubicación en zonas o ubicación geográfica, ya que teóricamente se supone que no habrá mucha variaciones de las velocidades de transmisión y recepción de los datos entre el servidor y las estaciones; siguiendo siempre la relación de 4 estaciones por módems, como dicen las indicaciones de los fabricantes de dichos equipos, se hará una tabla de asignación de los clínicas con el horarios de conexión para cada una de ellas acorde con las necesidades y la cantidad de información que ellos necesiten transmitir a la Oficina Central.

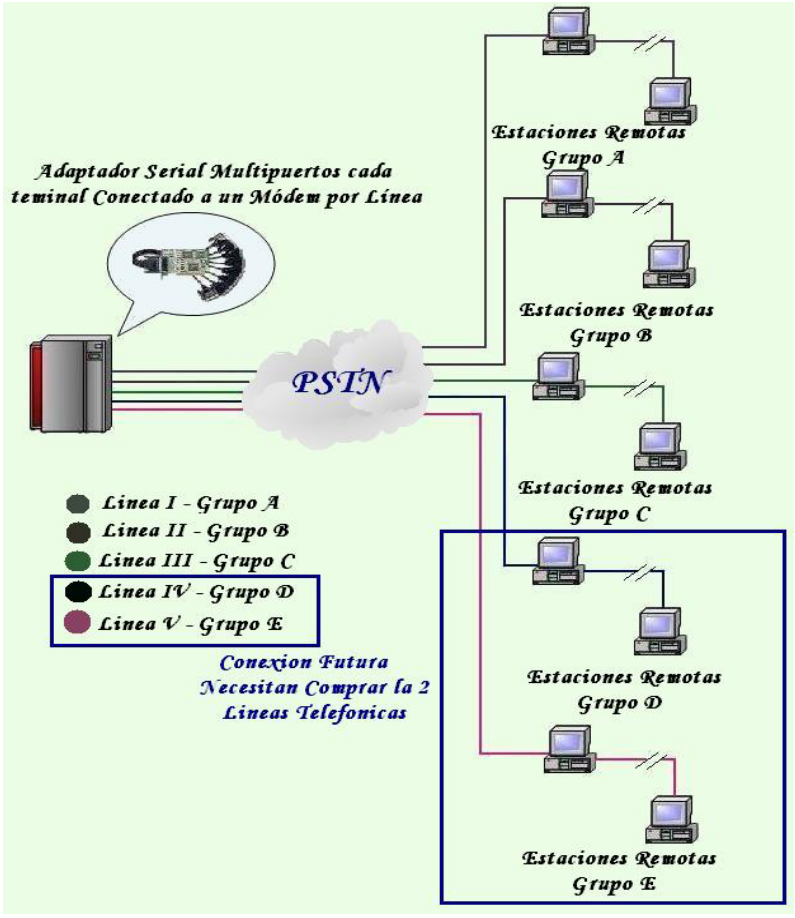


Figura 4.5: Esquema de Configuración con el Adaptador

4.4.3 Comunicación Entre Servidores

Como se dijo con anterioridad existe un servidor que maneja todo el todas las cuentas y servicios con los que esta trabajando la institución hasta el momento (Servidornt), después nos disponemos a instalar un servidor Linux con el servicio de acceso remoto, cuentas de usuarios remotos, con las opciones de autenticación y validación de las cuentas. Para que estos usuarios pueden acceder al servidor NT y aprovechar los recurso de este, se necesita establecer una conexión desde las estaciones remotas hasta dicho servidor, pasado por el servidor Linux, para esto se dispone establecer un mismo lenguaje de comunicación entre ambos servidores. Para establecer este entendimiento se plantea la instalación de NIS (Sistema de Información de Red) por parte de Linux y SFU (Servicio para UNIX) por parte de Windows, ya que estas aplicaciones manejan el mismo protocolo NFS (Sistema de Archivo de Red), que permite que exista una comunicación transparente entre las dos plataformas

permitiendo que las estaciones remotas que están conectadas al servidor Linux puedan tener acceso al servidor NT y compartir los recursos.

***Figura 4.6*: Comunicación entre los servidores**

4.4.4 Costo

Un punto clave en la propuesta es “Costo”, ya que la licencia de Suse Linux es gratuita, pero incurre en costos al momento de instalación, configuración y activación de todos los servicios que se necesitan implementar. Como sistema de redes no necesitaremos ningún tipo de software adicional para implementar el Servicio de Acceso Remoto y la seguridad en el dominio de PROFAMILIA. Por la comodidad que tiene el sistema el administrador puede configurar los servicios de la forma más eficiente, conforme con los requerimientos y necesidades de la institución. También se incurrirán en gastos al momento de la compra de hardware, ya que se necesita comprar una tarjeta Adaptadora multipuertos (ya escogida por nosotros tomando en cuenta las característica y eficiencia de la misma) y 5 módems de 56Kbps que sean compatibles con la tarjeta Adaptadora multipuertos, para realizar la comunicación se necesita ampliar las cuñas telefónicas de 3 líneas existentes a 5 líneas para cubrir a todas las estaciones remotas. Todo el estudio de costo esta más detallado en el Capitulo V de este trabajo.

4.4.5 Servicio de Acceso Remoto en PROFAMILIA

Como se dijo con anterioridad se el servidor que esta designado para realizar la conexión RAS es el equipo que esta como servidor Unisys, al cual se le recomienda realizar algunos cambios detallados mas abajo para asegurar los requerimientos del nuevo sistema operativo, al realizar la instalación de Suse se activara y configurará el servicio de Acceso Remoto junto al protocolo pppd para realizar la conexión de las estaciones remota, validando o rechazando las peticiones de los usuarios que solicitan la entrada al servidor. Una vez configurado pppd y RAS, se crearán y activarán las cuentas de cada uno de los usuarios, además de activar las normativas de autentificación y seguridad de la misma. Por parte de hardware se instala y configura el adaptador multipuertos (que los controladores tiene soporte en Suse Linux), luego se conectaran al Adaptador Multipuertos un juego de 5 de módems que a su vez estarán conectados a cada una de las líneas telefónicas (asumiendo 2 líneas que hacen falta existan) para recibir las peticiones de acceso de los clientes RAS, que ya estarán creados con anterioridad respetando las reglas, estatutos y criterios de conexión que seguirá el nuevo sistema y de la institución.

- **Servidor de Acceso Remoto:** Tomando en cuenta el inventario Hardware y software realizado en la Clínica Central, para servidor es recomendado utilizar el equipo de Bases de Datos Unisys (Bosht_221, ver Tabla 1.2) que esta actuando como un Member Server de la red, al cual se deben realizar algunos cambios, como el aumento en la capacidad de disco duro (compara uno de mayor capacidad), este equipo a criterio nuestro es ideal para soportar el trafico de las conexiones remotas, además que es posible habilitar los servicios de acceso remoto, enrutamiento, mensajería electrónica, autentificación y seguridad, de acuerdo a las requerimientos de hardware que tiene el sistema.

- **Estaciones Remotas:** Actúa como cliente remoto, serán equipos clones entre Pentium II Y III, que son equipos que están dentro del inventario de la institución y son recomendables por ser capaces de mantener una comunicación confiable en términos de conexión y velocidades de transmisión con el servidor, estos equipos serán activados como clientes remotos y serán responsables de la comunicación de las

clínicas con la Oficina Central. Estos clones manejan sistemas operativos como: Windows 98, Windows 98SE, Windows 95 (A y B), y Windows Milenium (mas especificado en el Inventario descrito en el Apéndice A), para los cuales es posible activar el cliente de servicio acceso remotos. La única alternante es verificar la compatibilidad de los Módem que tienen instalados dichas maquinas y remplazar los que no tienen compatibilidad con el adaptador Multipuertos.

- **Información a Transmitir:** Informes, cartas, estadísticas, etc. Ósea, transmisión únicamente de datos.

Protocolos para Acceso Remoto

Para hacer el RAS, se necesita configurar los protocolos a nivel de Wan y Lan, como sigue a continuación:

- **WAN:** Suse Linux soporta los siguientes protocolos de acceso remoto: PPP, SLIP, Protocolo RAS.

- **LAN:** Soporta aquellos protocolos para clientes remotos que permiten conectarse que son: TCP/IP, IPX, AppleTalk., NetBEUI.

4.4.6 Mensajería

Junto con el servicio de acceso remoto se ve la necesidad de implementar un servidor de mensajería bajo Sendmail que actúa como agente de transporte de correo (Mail Transport Agent - MTA), justificado por la razón de que el sistema de mensajería que tiene la institución que es Microsoft Exchange, no es compatible en Linux, por lo que hay que migrar el servidor de correo hacia Sendmail, creando la base de datos de usuarios locales y remotos dentro del mismo.

Servidores de correo electrónico seguros: La información de correo electrónico, nombres de usuario, contraseñas y mensajes, se puede interceptar y ver sin que tenga

conocimiento el servidor o el cliente de correo. Al usar los protocolos estándar en cualquier red entre el cliente y el servidor remoto, la información puede ser vista fácilmente. La mayoría de los agentes MUA de Linux están diseñados para comprobar el correo mediante SSL compatible con servidores de correo para cifrar los mensajes, de modo que se devuelvan y envíen en la red. Los protocolos estándar seguros tienen números de puerto conocidos que MUA utiliza para autenticar y descargar los mensajes. Linux utiliza bibliotecas SSL externas para ofrecer un cifrado eficaz y proteger las conexiones. Puede solicitar a una Autoridad de certificados, un certificado SSL o crear un certificado firmado propio para obtener las ventajas de una comunicación cifrada con SSH.

4.4.7 Seguridad y Autenticación

Esta propuesta basada en Linux, presenta un alto nivel de seguridad debido a la complejidad del sistema de seguridad que tiene Linux, por esa razón se ha tomado en cuenta realizar la autentificación y validación de los usuario remotos a través de Security Shell, ya que permite activar los registros de los usuarios con autentificación y comunicación de datos de una forma segura con a través de algoritmos criptográficos con acceso al servicio Remoto (RSA), además tiene un control de usuarios a través de ficheros con el que se actualizaran la tablas de usuarios para mantener segura la comunicación. También este servicio ofrece al cliente seis métodos distintos de validarse en el servidor, por lo cual los usuarios manejaran dos métodos de para autentificarse. Esto mejorara grandemente la privacidad de la institución con respecto al manejo de su información.

Políticas de Seguridad

PROFAMILIA necesita intercambiar información con las clínicas remotas para mejorar la organización y la confiabilidad de esta comunicación, para esto se plantean políticas de seguridad referenciada de las PSI de UNIX[40], tomando en cuenta los siguientes aspectos:

40 Mejor detallado en la tabla A6 en Anexos, exctraida del documento PROBLEMAS DE SEGURIDAD EN EL MUNDO UNIX – LINUX de Pedro Gómez Ochoa

- **Políticas de Passwords**
- **Autentificación y Validación de Usuarios Remotos**
- **Políticas de Backups**
- **Determinación de niveles de Acceso**

También se toman en cuenta la Seguridad Lógica a nivel de Software que son:

- **Minimizar los ataques de Virus Informáticos**
- **Minimizar los ataques o intercepciones de terceros**
- **Estar al tanto de vulnerabilidades y Mejoras a software con fallas**
- **Desactivar todos los servicios que no se utilicen**
- **Cerrar puertos no utilizados**
- **Contar con reglas de Firewall (ipchains iptableswrappers)**
- **Auditar permanentemente la red**

Autenticación Kerberos

Existe otra opción de autentificar y validar a los usuarios remotos, por lo que también se propone una segunda opción de seguridad que es la Kerberos que mejorar la seguridad obtenida con Security Shell. La autenticación Kerberos que esta integrado en la versión de Suse Linux 8.0, por lo que no representa ningún gasto adicional para la institución. Este procedimiento mejora la eficiencia en las opciones de validación de usuarias y se realiza a través de un proceso de entrega de tickets que se envía de forma encriptada, para esto Kerberos manejara una base de datos que será creada y almacenada con la información de lo usuarios de la institución, aquí cualquier tickets o petición de entrada son comparados, aceptados o rechazado por Kerberos. Esta alternativa esta pensada para mejorar el sistema actual, con un mínimo de condiciones que limiten la implementación del acceso remoto, tomando en cuenta que las dos partes de la red (Estación Remoto – Servidor), y la configuración de los protocolos de autenticación.

Capítulo V:

Mediciones y Costos

Capítulo V: Mediciones y Costos

En este apartado se tratara de evaluar ***Cuantitativamente*** si una implantación RAS (usando una PSTN como red de transito) para PROFAMILIA es viable en términos de costos, confiable para transmitir los volúmenes de datos requeridos y si es eficiente en términos de las aplicaciones o servicios que se requieren.

Antes de desarrollar este apartado, aclaramos que no estamos haciendo un completo estudio sobre el uso de la red PSTN de ENITEL mediante un servicio RAS, puesto que esto realmente implica más que hablar de configuraciones y equipos de interfaces. Lo que queremos decir es que en la actualidad el crecimiento de la demanda de accesos a Internet y la transferencia de grandes volúmenes de datos con características de aplicaciones multimedia, mediante el uso de este tipo de infraestructura a venido a crear debates sobre la regulación de su uso para estos tipos de trafico, formas de establecimientos de precios y condiciones para su interconexión con diferentes tipos de redes y por tal razón nuestro estudio estará mas enfocado a la calidad del servicio que pueda brindarnos.

Lo anterior significa que aun siendo una red con iniciales de “PUBLICA” realmente no significa que podemos utilizarla como mejor nos convenga. Hay que recordar que los operadores de telefonía tradicional cada día están diseñando nuevas estrategias que logren evitar que su red de voz, sea utilizada para el trafico de datos multimedia, ya que este ultimo consume recursos de transmisión y conmutación altamente costosos, puesto que es evidente que las características de sus redes no fueron diseñadas para este tipo de trafico.

5.1 Alcance de Mediciones

¿Que vamos a medir y porque? Se deben reconocer algunas de las características principales de nuestra red que servirá como enlace WAN, así como los criterios que nos llevan a identificarla como una alternativa. De esta forma determinaremos hasta que niveles de evaluación podemos aplicar a este tipo de enlace. La razón de tratar de utilizar la red de ENITEL en lugar de seguir utilizando los ISP que actualmente se utilizan, se deriva de los siguientes criterios:

- Reducir los costos de conexiones.

- La cantidad de tiempo de conexión que las Oficinas Regionales utilizan y requieren, no son mayores de una hora por día, es decir que no se necesitan arrendar líneas de conexiones permanentes (usadas las 24 horas al día y de altos costos).

- El costo beneficio que reciben las Oficinas Regionales del servicio actual brindado por los ISP, ya no satisface sus necesidades de operaciones informáticas (actualización semanales de los inventarios y flujos de caja a un sistema de base de datos ubicada en la Oficina Central y mensajería electrónica directa e interna).

- La tasa o el volumen de datos que se requieren manejar no sobre pasa la necesidad de un ancho de banda (BW) mayor de 64Kbps o 128Kbps.

- No se requieren altos niveles de disponibilidad inmediata (son aceptables tiempos de establecimientos de llamadas de 5 a 10seg que teóricamente presentan las PSTN), ni que sean extremadamente confiables en los enlaces requeridos.

- Las trayectorias que cubrirán las señales electromagnéticas no sobre pasan el orden de los miles de kilómetros, esto es importante por el hecho de los retardos de propagación que sufren los datos.

Los criterios anteriores destacan que, la institución técnicamente no urge de enlaces dedicados con altas capacidades de ancho de banda y que un enlace WAN con las características teóricas que ofrece la red PSTN de nuestro país podrían ser aceptables técnicamente para cumplir sus necesidades.

5.2 ISP VS PSTN

Utilizando los ISP, las trayectorias por donde fluyen los datos es distintas a las que tomarían en la red PSTN, al momento que las Oficinas Regionales necesiten transmitir

(correos electrónicos y peticiones para acceder a sitios del Internet) o recibir (correos electrónicos y información del Internet) datos.

5.2.1 Utilizando una Conexión ISP

Se establece un conexión corta y local (los retardos de propagación en este tramo son cortos), que tiene como origen la Oficina Regional y como destino el POP (Punto de Presencia) del ISP, una vez hecha esta conexión el ISP envía los datos a través de líneas dedicadas (existe un ancho de banda reservado para el trafico en cuestión) hacia un punto de su red que tenga conexión con un IXP (Punto de intercambio Internet, Internet Exchange Point) para proporcionarle acceso a Internet o acceso a un servidor de correo donde existen sus cuentas de correo.

En este caso tenemos una red confiable y donde los recursos para cada cliente ya han sido reservados para ofrecerles cierta calidad en el servicio. Sin embargo mantener este servicio requiere un costo que se suma a la tarifa del tiempo que permanece ocupada una línea telefónica convencional y que como mencionamos anteriormente ya no satisface las nuevas necesidades de la institución.

5.2.2 Utilizando una Conexión PSTN

La trayectoria del flujo de datos es muy diferente por su comportamiento de conmutación de circuitos.

Es una red con estas características, las trayectorias que tomara el flujo de datos varia con cada establecimiento de llamada, es una red en la que no podemos reservar recursos dinámicamente cuando hacemos un simple establecimiento de llamada (no es una red de paquetes o mensajes). Sin embargo PSTN al contrario de Internet esta diseñada para una principal aplicación (voz) y todas las conexiones de esta requieren exactamente el mismo nivel de servicio, por lo tanto el ancho de banda del canal es asignado al usuario incluso antes de que pueda fluir la conversación, y en el caso que no halla recursos para una

llamada, esta es rechazada y no se sacrifica la calidad de los demás usuarios. Fue diseñada para cumplir con este QoS desde el principio.

Existen variabilidades de anchos de banda a lo largo de una ruta (origen-destino) y hay una mezcla de tráfico a través de los troncales entre oficinas de conmutación regionales (multiplexación por división de tiempo utilizando la técnica PCM). Sin embargo esta red posee una gran capacidad debido a su modernización iniciada en 1991 y según un documento elaborado por la Dirección de Desarrollo de Telcor, la red de telefonía publica de ENITEL a gradualmente mejorado su infraestructura de tal manera que desde el año 1991 al 2002 ha logrado que el 99% de su red sea digital y su capacidad de usuarios aumente, esto motiva el intentar utilizarla.

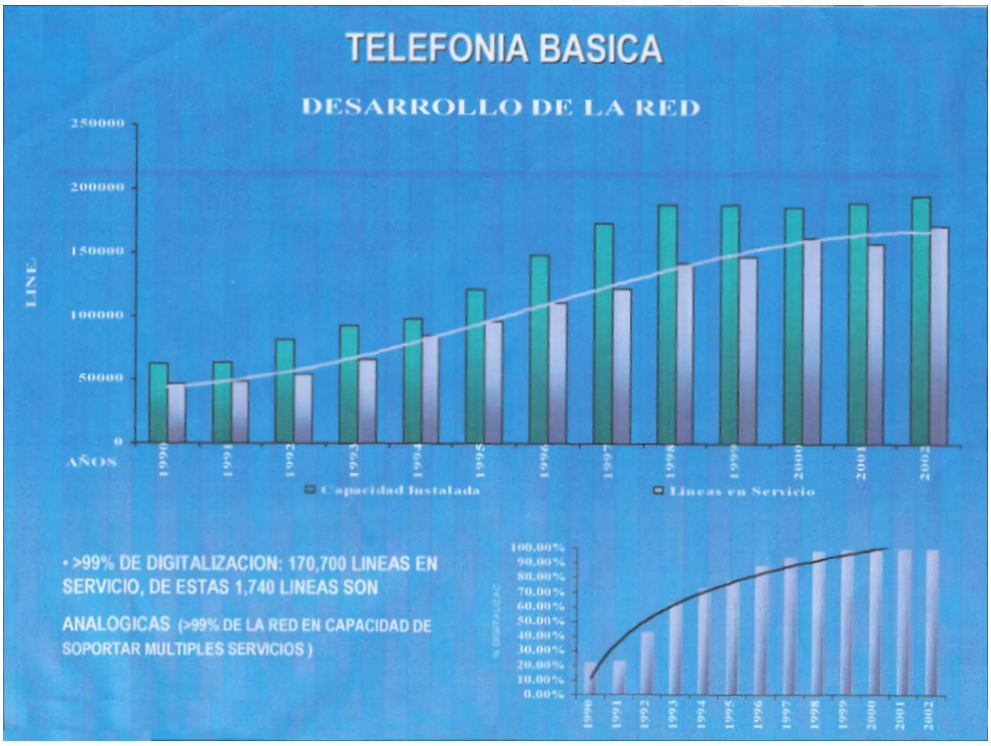


Figura 5 .1: Desarrollo de telefonía básica en Nicaragua

Considerando esta red, la trayectoria que tomaría el flujo de datos tendría la siguiente secuencia de establecimiento: Cada Oficina Regional establecería una llamada local a la correspondiente oficina de conmutación telefónica regional y de aquí un enlace troncal hacia la oficina de conmutación que domina al número telefónico destino (en este caso Oficina Central), la llamada será atendida por un servidor RAS que servirá de puente entre el usuario remoto y todos los servicios y recursos que le sean brindados por la LAN de PROFAMILIA .

El costo será solamente el tiempo que se permanece ocupada la línea, sin embargo aun con las digitalizaciones de los equipos de conmutación siempre estaremos limitados por el bucle local con capacidad de 29.9016 kbps (Claude Shannon).

$$C = W \log_2 (1 + S / N)$$

C = Capacidad de Canal
W = Ancho de Banda de Canal
S/N = Relación de Señal a Ruido

Figura 5.2: Fórmula de Shannon

Sin lugar a dudas, el mecanismo de transferencia de datos entre las diferentes oficinas regionales y la oficina central de PROFAMILIA a través de un ISP es limitado en términos de las nuevas necesidades de servicio que esta requiere.

Hasta este punto hemos logramos concluir que existen dos alternativas de enlace que difieren una de la otra por su nivel de confiabilidad y capacidad para prestar condiciones previamente reservadas que garantizan la transmisión de cualquier flujo de bits y por su costo de uso. El decidir una de otra, es una decisión tanto técnica como económica y merece este estudio.

Ahora veamos como y que podemos evaluar para estar seguros que tendremos prestaciones de trafico confiable. Esta claro que necesitamos de una cuantificación de parámetros que ayuden como soporte a nuestras razones de elección de este tipo de red de comunicación.

Recurrimos a un concepto denominado por la ISO como QoS (Quatity Of Service, Calidad de Servicio), y este termino se entiende, como la capacidad que tiene un sistema para asegurar con un grado de fiabilidad preestablecido, que se cumplan los requisitos de trafico, en términos de perfil y ancho de banda, para un flujo de información dado. De este modo se establecen clases de servicios para tratar de forma diferente los flujos de tráfico, y por supuesto se incrementan costos adicionales a los del best Effort[41].

41 Con el servicio best-Effort, no hay garantías totales ni parciales de un servicio. No se requiere especificación de parámetros QoS o cotas en formas determinísticas o probabilísticas.

El QoS es un concepto muy utilizado a nivel de capa de red, donde los equipos enrutadores poseen protocolos que ayudan a gestionar y diferenciar los flujos de trafico (conjuntos de paquetes que van de un origen a un destino), con el propósito de reservar recursos para tráficos que se consideren mas prioritarios que otros, y de esta forma garantizar una calidad de servicio. Por ejemplo, un flujo de tráfico de una aplicación como videoconferencia tendría más prioridad de usar los recursos de la red por donde transita que una aplicación como correo electrónico.

En conclusión, QoS nos puede revelar que tan buenos son los servicios ofrecidos por una red (en términos de capacidad de enrutamiento), para un determinado flujo de información y de esta manera podríamos saber si hacen falta mas recursos, que tipo de recursos y en que puntos de la red. La medición de QoS es posible porque se pueden diferenciar los flujos de información por los parámetros cuantitativos que requieren.

Los parámetros principales que pueden medirse son: Confiabilidad, retardo, fluctuación de retardo y ancho de banda. En la siguiente tabla se pueden observar un ejemplo de niveles de estos parámetros que se requieren por cada una de las siguientes aplicaciones, para que se puedan garantizar recursos de la red, y así tener un mejor desempeño cuando se prestan estas aplicaciones.

Aplicaciones	Confiabilidad	Retardo	Fluctuación	Ancho de banda
Correo electrónico	Alta	Bajo	Baja	Bajo
Transferencia de archivos	Alta	Bajo	Baja	Medio
Acceso a Web	Alta	Medio	Baja	Medio
Inicio de sesión remota	Alta	Medio	Media	Bajo
Audio bajo demanda	Baja	Bajo	Alta	Medio
Vídeo bajo demanda	Baja	Bajo	Alta	Alto
Telefonía	Baja	Alto	Alta	Bajo
Video, Tele-conferencia	Baja	Alto	Alta	Alto

Tabla 5.1: Niveles de QoS para Aplicaciones

En la tabla anterior, podemos observar que las primeras tres aplicaciones son los servicios que la institución desea extender a sus oficinas remotas con la implantación de un servidor RAS, así mismo se muestran los niveles que deben alcanzar los parámetros QoS mencionados. Estos niveles en los parámetros de las aplicaciones son una referencia al

momento de decidir si la red PSTN la cual utilizaremos como red de transito tiene la capacidad de proporcionarnos el soporte para los flujos de trafico requeridos.

Debemos tomar muy en cuenta que este concepto es implementado en sud-redes de comunicación donde la ruta que toman los flujos de información, es una interconexión de equipos enrutadores que trabajan al nivel de capa de red y que cuentan con capacidades de hardware y de software de control sobre los paquetes de datos que pasan por ellos y por lo tanto se le puede aplicar el concepto de gestión de QoS (reservar recursos).

Mientras que para una red de tipo conmutación de circuitos (PSTN) el concepto de reservar o gestionar recursos a través de una ruta de enlace no es posible hacerlo en forma dinámica, sino de forma estática, es decir que la única forma de reservar un recurso es por medio de la realización de un contrato de tipo servicio permanente para el usuario que lo contrata.

Sin embargo podemos seleccionar ciertos parámetros de QoS en una red PSTN, para evaluar el tipo de servicio (best Effort) que provee un simple canal de línea telefónica. Es decir podemos aplicar de forma virtual este concepto de calidad de servicio y de esa manera decidir si las condiciones que se prestan son favorables para los propósitos de la institución.

5.3 Parámetros a Medir

Antes de indicar que parámetros vamos a medir, es necesario saber a que nivel del modelo de referencia OSI haremos las mediciones, puesto que este mismo nos indicara los parámetros que tomaremos en nuestras pruebas de conectividad.

Como un primer paso a la parametrización, se debe considerar el QoS como un aspecto vertical de toda la arquitectura, es decir, debe estar presente a muchos niveles, por ello el primer esquema de división es a nivel de QoS.

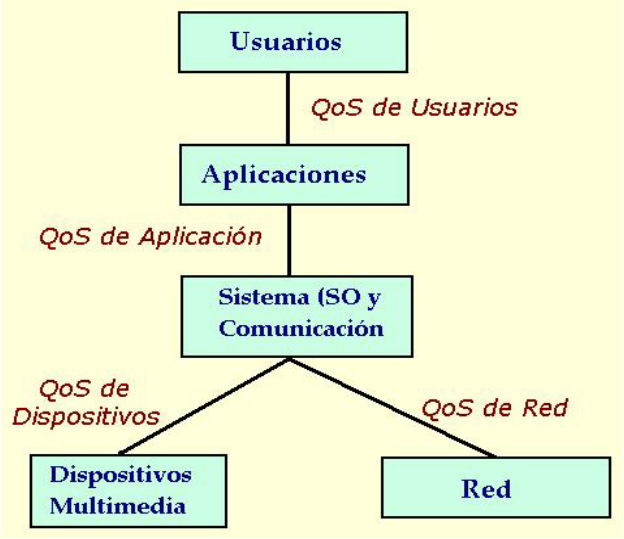


Figura 5.3: Niveles de Qos

Como puede observarse en la figura anterior, cada nivel posee determinados parámetros QoS que pueden evaluarse para determinar el desempeño de dicho nivel.

En nuestro caso los parámetros QoS, que podemos medir serán los correspondientes a la capa de enlace de datos del modelo de referencia OSI y no la capa de red. Por la sencilla razón, que la capa de red es la encargada de llevar paquetes de datos de un origen hasta un destino, utilizando su conocimiento de las estructura de la subred de comunicaciones y que a su vez esta conformada por una variedad de equipos de enrutamiento. En contraste con nuestra subred de comunicaciones (PSTN) que carece de este tipo de equipos que pueden diferenciar los paquetes, y que posee equipos de conmutación de circuitos que tiene como objetivo formar un enlace físico permanente(túnel) para lograr la unión de dos puntos distantes.

Además en la capa de enlace de datos se encuentra nuestro principal protocolo (PPP) utilizado para el establecimiento del servicio de acceso remoto. En este sentido esta capa maneja tramas de extremo a extremo sobre un enlace punto a punto, teniendo más acercamiento con los problemas que se dan en las comunicaciones a bajo nivel.

Recordemos que la capa de enlace de datos, trata de brindar servicios a la capa de red y que si en este nivel las tasas de errores en los envíos y recepciones de tramas son altos, el trabajo de recuperación de datos debido a errores en las líneas que realizan las capas superiores a la capa de enlace de datos pueden ser inútiles.

En consecuencia de lo expuesto anteriormente, definimos a la capa de enlace de datos como el punto de medición y que los parámetros QoS a medir serán:

- ***Throughput (cantidad de datos que pueden enviarse en un período de tiempo)***
- ***Lost packet o Error Packet (paquetes perdidos o paquetes erróneos)***
- ***Número de intentos para conectarse con el servidor RAS***
- ***Tiempo en que se establece la conexión RAS***
- ***Frecuencia de cortes ajenos al usuario***
- ***Utilización del ancho de banda (BWr/BWt)***

La evaluación de todos estos parámetros determinara la calidad de servicio best Effort que proporciona la infraestructura de la red PSTN y aunque estos resultados no sean relevantes para las ya reconocidas teorías sobre las máximas capacidades que posee un medio guiado del tipo usado en este tipo de redes, para la transmisión de datos digitales sobre señales analógicas, podremos observar detalles que nos ayuden de alguna manera a tratar de modelar el flujo del trafico futuro con el objetivo de obtener transmisiones de datos con una calidad e eficiencia moderada y con el menor costos posible al utilizar las líneas telefónicas, ya que el tiempo de uso incurre en los costos, siendo este un factor decisivo al momento de decidir.

Hay que recordar que si logramos evaluar que es factible usar una línea de este tipo de ancho de banda, podremos sustituir los ISP actuales y reducir los costos de llamadas por módem para cada una de las oficinas remotas, y aunque esta reducción de costos sea pequeña en términos macro, su sumatoria anual podría dar como resultado un monto que puede convertirse en una inversión generadora de ganancias para la institución a largo plazo.

Definido el alcance de las pruebas, nuestro objetivo principal es: Utilizar parámetros QoS, para evaluar el Best Effort de líneas PSTN, comparar los resultados obtenidos con los niveles QoS de al menos una de las aplicaciones que se quieren implantar y demostrar su factibilidad técnica y económica.

5.4 Etapas de Desarrollo de las Mediciones

Elección de los puntos donde se harán las pruebas y el tamaño de las muestras. Para obtener un buen grado de confianza en las pruebas y obtener resultados satisfactorios para la institución, realizaremos las pruebas de conectividad desde los puntos remotos más relevantes, dados sus niveles de atención de usuarios (criterio de selección) puesto que ellos manejan mayores volúmenes de información y trataran de consumir el máximo desempeño que pueda proporcionar la infraestructura PSTN. Además, la distribución geográfica de estos puntos incluye una buena proporción de las cabeceras departamentales, esto es muy importante ya que las mediciones se realizan a una variedad de distancias que al final de las mediciones contribuyen a obtener medias muéstrales de los parámetros medidos aproximadas a los valores reales y máximos que se pueden obtener para la zona del pacifico del país.

Los puntos remotos elegidos para realizar las mediciones de los parámetros de QoS antes expuestos y ordenados de acuerdo a los promedios de usuarios que se atienden mensualmente, están resumidos en la siguiente tabla[42].

Ubicación De Los Puntos De Mediciones Estratégicos			
No. Visita	**Origen**	**Destino**	**Numero De Usuarios**
1	Managua	Boaco	2,400
2	Managua	Juigalpa	1,338
3	Managua	Matagalpa	1,163
4	Managua	Chinandega	1,125
5	Managua	Estelí	1,120
6	Managua	Granada	1,100
7	Managua	Rivas	964
8	Managua	Jinotega	700

Tabla 5.2: Programa de Visitas

Dados los puntos remotos donde se concentran los mayores volúmenes de información y de usuarios, solo nos resta determinar el tipo de muestreo y la cantidad que debemos observar con el propósito de medir los parámetros de QoS que nos interesan.

42 La información de la tabla es proporcionada por el departamento de Planificación Evaluación y Desarrollo de PROFAMILIA, coordinada con el departamento de TI. En anexos puede observarse el calendario de visitas a las oficinas remotas y costos.

El tipo de muestra que analizaremos son tramas que se intercambian entre puntos remotos que utilizan PP como protocolo de enlace y negociación de vínculos punto a punto. En la practica estas tramas PP (punto a punto) poseen una aproximado tamaño de MTU de longitud máxima de 1500 bytes, y de las cuales podemos obtener el comportamiento de los parámetros QoS del best Effort de la red PSTN para el tipo de transmisión de datos. Debido a que necesitamos confianza en los resultados de las mediciones, tomaremos ¼ (15 minutos de muestro de tramas PP) del espacio muestral que hemos definido como una hora(60 minutos), ya que este espacio muestral es el intervalo promedio de utilización de las conexiones de marcado que hacen las oficinas remotas.

Esta proporción de tiempo de muestreo los deducimos asumiendo que el tiempo de uso de la línea telefónica por cada oficina remota es aproximadamente una hora por día, así calculamos cuantas tramas PP con MTU= 1500 bytes, se transmiten en este periodo de tiempo.

1 byte = 8 bits
MTU PP = 1500 bytes
Capacidad de transmisión del canal = 29.9016 kbps
Tiempo de uso de la línea telefónica = 3600 seg x dia
El # de tramas PP, transmitidas en una hora es
≈ (29.9016 kbps/seg)(3600seg)
≈ (107,645.76 kbit)/(8 bits)
≈ (13,455,720 bytes)/(1500 byte)
≈ 8,970 unidades

El estimado de tiempo de uso de la línea telefónica es proporcionado por el departamento de tecnología de la información de PROFAMILIA.

El total de los 15 minutos, será dividido en cinco períodos de muestreo de 3 minutos con intervalos de separación de 3 minutos entre la toma de una y otra muestra.

La selección del tamaño de la muestra se realiza por el método de muestreo no aleatorio o de juicio, basado en los conocimientos que tenemos sobre la poca variabilidad que tenemos en las velocidades de transmisiones de datos que se presentan en una línea telefónica convencional. Además este método es muy utilizado como un muestreo piloto que podría ser usado para decidir como seleccionar un muestreo aleatorio en el caso que otra persona decida hacerlo.

El muestreo aleatorio no fue utilizado por la falta de estimadores estadísticos anteriores a nuestras mediciones, que pudieran orientarnos en la estimación del tamaño de las muestra de tramas PP, por tanto la selección de la muestra a través de las ecuaciones de Intervalos de confianza para medias muéstrales o poblacionales así como desviaciones muéstrales y poblacionales fueron inútiles para nuestro propósitos de toma de muestras.

No hay que olvidar que las tramas a muestrear PP son los generadores de los parámetros QoS que buscamos por tanto cada trama PP es un elemento fundamental en el muestreo de estos parámetros, convirtiéndose así cada parámetro en una variable aleatoria a la cual le calcularemos su media muestra. Considerando que la media muestral de estos parámetros es una estadística, entonces tienen una distribución de probabilidad, para la cual no conocemos su forma de distribución de frecuencia de la población. Por tanto dado que se desconoce la distribución de la población de cada uno de los parámetros QoS, nos apoyamos en el principio del teorema del limite central[43], para establecer los 15 minutos de muestreo antes mencionados y que sin duda sobrepasan un numero de n-tramas > 30, que hace que nuestras inferencias estadísticas sean muy confiables.

5.4.1 Plan de Realización de Pruebas

El objeto de estas pruebas es medir parámetros QoS, para evaluar el Best Effort de líneas PSTN y comparar los resultados obtenidos, con los niveles QoS de las aplicaciones que se quieren introducir, así como demostrar su factibilidad técnica y económica.

5.4.2 Descripción de la Prueba de Conectividad

El método de realización de las pruebas se basa sobre aplicaciones cliente / servidor, específicamente ejecutando el servicio de acceso remoto y mensajería electrónica.

La prueba consiste en tratara de medir los parámetros QoS usando un software que capture un flujo de tramas PP que se genera entre un servidor de acceso remoto y un cliente

43 La relación existente entre la forma de la distribución de la población y la forma de la distribución muestral de la media recibe el nombre de teorema de l límite central. Este teorema garantiza que la distribución muestral de la media se acerque a las distribuciones normales a medida que crece el tamaño de la muestra.

de acceso remoto, al momento en que el cliente remoto esta realizando una transferencia de datos a través del servicio de mensajería electrónica.

Para proceder a las mediciones de forma ordenada y efectiva ante cualquier factor fortuito que pueda darse y que no retrase la obtención de los resultados de la misma, definiendo los requerimientos de hardware y software necesarios en las configuraciones plantadas para las realización de mediciones.

5.4.3 Definir Software y Hardware utilizados para las Pruebas de conectividad

En la plataforma Windows NT Server 4.0

Software

Sistemas Operativos

Windows NT Server 4.0

Windows98 Segunda Edición

Software extra

Microsoft Exchange 5.5

Etherpeek versión 4.2.0.4

Los requisitos de hardware corresponden a los requerimientos de los equipos PC y accesorios que utilizaremos en la realización de las pruebas de mediciones y están divididos para las plataformas Windows NT Server 4.0 y SuSe Linux 8.0, con su respectivo cliente remoto.

Hardware

Parte servidor.

- Servidor UNISYS como servidor de acceso remoto (sus especificaciones físicas se encuentran en el capitulo I de este documento).
- Servidor COMPAQ PROLIANT ML350 “Servidornt”, donde crearemos una cuenta de correo electrónico (sus especificaciones físicas se encuentran en el capitulo I de este documento).
- Módem U.S Robotics modelo 0710 (Especificaciones están en apéndice A).

- Línea telefónica analógica convencional.

Parte cliente.

- Computadora LapTop marca Dell, modelo Latitude XPi, 133 Mhz, 32 RAM.
- Módem interno de 56 kbps.
- Línea telefónica convencional

En la plataforma Linux Suse 8.0

Software

Sistemas Operativos

Suse Linux 8.0 (Servidor Ras)

Windows NT Server 4.0 (Servidornt)

Windows98 Segunda Edición

Software extra

Send Mail

Etherpeek versión 4.2.0.4

Parte servidor.

- Computadora Clon (750 MHz de Procesador, 128 de RAM, 20 de Disco Duro) como servidor de acceso remoto.
- Servidor COMPAQ PROLIANT ML350 “Servidornt”, que estará funcionando como servidor primario (sus especificaciones físicas se encuentran en el capitulo I de este documento).
- Módem PCTel – Modelo PCT789 – 9912.
- Línea telefónica analógica convencional.

Parte Cliente.

- Computadora LapTop marca Dell, modelo Latitude XPi, 133 Mhz, 32 RAM.
- Módem interno de 56 kbps.
- Línea telefónica convencional

5.5 Resultado de Mediciones.

En la siguiente tabla se muestran los resultados obtenidos a través de las pruebas de conectividad que se realizaron dentro del periodo estimado de visitas a los puntos remotos.

Parámetro	Boaco	Juigalpa	Matagalpa	Chinandega	Estelí	Granada	Rivas	Jinotega	Prom.
Throughput (Kbps)	29.54	28.90	29.88	30.99	31.20	32.22	29.00	30.34	30.25
% Error Packet	37.10	35.00	37.00	35.71	35.19	34.47	34.67	35.81	35.61
# Intentos de Conexión	2	1	2	1	1	1	2	2	2
Tiemp /Est de Conexión (Seg)	22	25	20	30	23	25	20	30	25
Frecuencia de Cortes	-	-	-	-	-	-	-	-	-
%Utilización del BW (BWr/BWt)	89.51	87.57	90.54	93.90	94.54	97.63	87.87	91.93	91.68

Tabla 5.3: Parámetros medidos de Qos

En la tabla se puede observar que los promedios de los parámetros medidos no difieren mucho unos de otros, aun cuando los puntos donde se obtuvieron los datos se encontraban en diferentes ubicaciones geográficas. Además se puede deducir que las condiciones técnicas de las conexiones punto a punto utilizando un servidor de acceso remoto propio pueden sustituir los servicios que les proporcionan los ISP a la institución.

Un dato muy importante es el Error packet que es un aproximado del 35.61% del total del flujo de datos en la línea física de transmisión. Este parámetro específicamente se refiere a las tramas ¨Runts¨, que básicamente es el porcentaje de tramas con una longitud menor de 64 Bytes (un valor ilegal dentro de la especificaciones 802.3 Ethernet). Es decir la presencia de estas tramas se refiere a fragmentos de colisiones que se dieron durante la comunicación entre ambos extremos, recordemos que las distancias en la línea física son muy largos y se producen retardos de propagación de la señales eléctricas que viajan por el, dando originen a que las estaciones que se encuentran en los extremos de la línea no escuchen a tiempo actividad en el la línea.

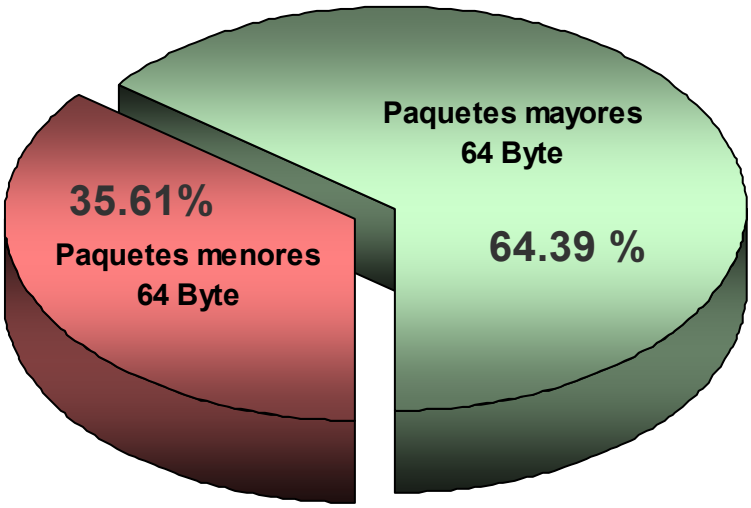


Figura 5.4: Porcentaje de Error Packet

Estas colisiones producen una perdida del ancho de banda del enlace, afectando considerablemente el desempeño del mismo cuando son por porcentajes muy altos, pero para estas pruebas se considera aceptable dada las distancias entre los puntos.

5.6 Comparación en Costos de Alternativa.

Estos costos son tomados de cotizaciones realizadas con distintos proveedores y tomando en cuenta parámetros establecidos para realizar la configuración de las alternativas.

Alternativa	Costo Licencia	Inst. / Conf. Servidor	Conf. 19 Estaciones	Costo Hardware	Totales
Windows NT Server 4.0	$ 0.00	$ 300.00	$ 475.00	$ 886.91	**$ 1,661.91**
Windows NT Server 4.0	$ 0.00	$ 300.00	$ 475.00	$ 1124.91	**$ 1,899.91**
Windows 2000 Server	$ 900.00	$ 300.00	$ 475.00	$ 1124.91	**$ 2,799.91**
Suse Linux 8.0	$ 0.00	$ 500.00	$ 475.00	$ 1124.91	**$ 2,099.91**

Tabla 5.4: Cuadro Costos De Las Alternativas Propuestas.

Los costos de la licencia solo se incluyen en la tabla los de Windows 2000 Server ya que es el único al que se le compraría dicha licencia, ya que Suse Linux 8.0, es gratuito y Windows NT Server 4.0 PROFAMILIIA ya cuenta con una Licencia vigente.

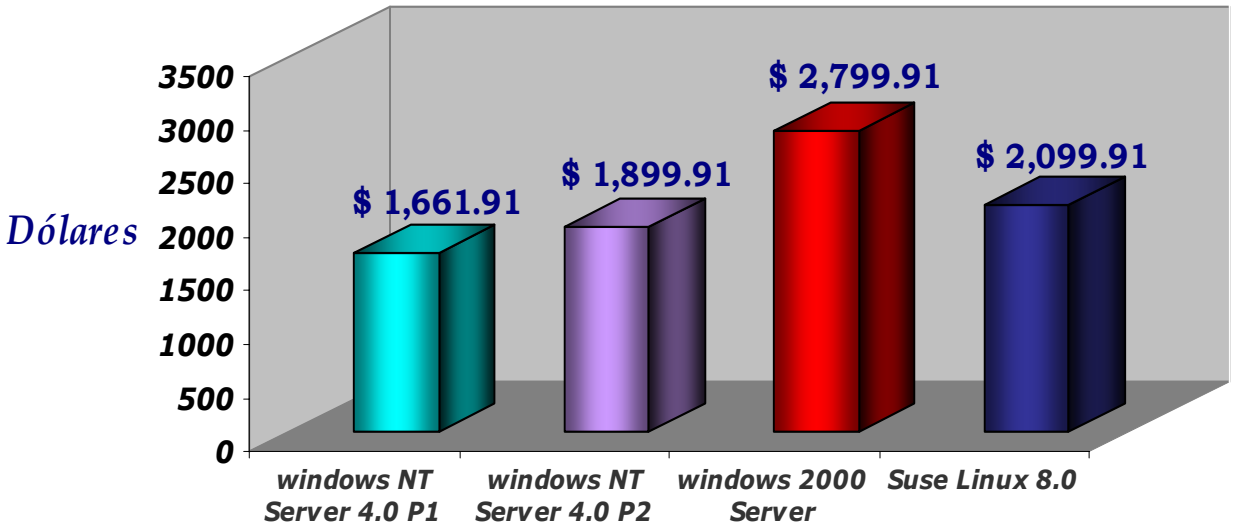


Figura 5.5: Costos de Implantación de las Alternativas Propuestas.

Vemos en la gráfica que los costos de implantación de las alternativas no exceden los tres mil dólares, por lo que consideramos que cada una de estas propuestas podría ser considerada para realizar la configuración del RAS en PROFAMILIA.

CONCLUSIONES

En base al estudio técnico y económico que se realizó en PROFAMILIA y tomando en cuenta la estructura actual de sistema de la red, tanto en hardware como los sistemas operativos que tienen hasta el momento se llegaron a las siguientes conclusiones:

- La plataforma tecnológica de PROFAMILIA reúne los requerimientos mínimos para activar el servicio de Acceso remoto y convertirse en su propio proveedor de servicios de red, logrando la integración de sus recursos materiales y humanos, reduciendo costos y mejorando los servicios que como institución ofrecen.

- De acuerdo a la naturaleza de la institución y el desarrollo de los sistemas Linux, valorados por su confiabilidad, junto con las mejoras en su entorno de red y costos de implantación as nuestro criterio es la opción más viable y factible para suplir las necesidades de comunicación que la institución tiene en estos momentos.

- Mediante las mediciones realizadas, concluimos que el desempeño de las líneas telefónicas para el establecimiento de las conexiones remotas, se encuentran entre los intervalos aceptables para este tipo de servicio de acuerdo a los parámetros de calidad de servicio.

RECOMENDACIONES

Para que la implementación del Servicio de Acceso Remoto trabaje de la manera más eficiente en la Institución, se recomienda:

- ❄ Incrementar los requerimientos de hardware de los equipos que funcionan como servidores de red, con el objetivo de mejorar la redundancia en el almacenamiento de los datos y estar preparados ante siniestros. Además esta mejora del hardware incrementa la capacidad de respuesta del sistema ante peticiones simultáneas de servicios.

- ❄ Utilizar la menor cantidad de protocolos de red que los usuarios remotos tendrán habilitados para correr en la Intranet, autenticar con el método mas seguro, no utilizar cuentas administrativas con permisos de acceso remoto a menos que se requieran, restringir a los usuarios remotos a servicios y recursos específicos, no utilizar programas de compresión de datos cuando se utiliza la compresión que ofrece el acceso telefónico de redes. Además de aplicar las políticas de seguridad mencionadas en las diferentes alternativas.

- ❄ Realizar un documento que contenga la secuencia y horas en que los usuarios remotos puedan solicitar conexión, con el propósito de tener mayores probabilidades de conexión y utilizar el servicio en las horas no pico de servicios telefónico.

- ❄ El arrendamiento de 2 líneas telefónicas mas, ya que hasta el momento solo cuenta con tres líneas lo que resulta limitado para la cantidad de estaciones remotas que se desean conectar, la cantidad de estaciones se toman en la relación de estaciones por Módem que es un parámetro que constante de 4 estaciones por módem.

- ❄ La compra de un Adaptador multipuerto en lugar de un pool de módems.

BIBLIOGRAFÍA

- Andrew S.Tanenbaum, ***Redes de Computadoras*** 3ª Edición, Editorial Pearson Educación, Naucalpan, México, 1996.

- Craig Zacker, **Redes Manual de Referencia,** 1ª Edición, Mc Graw Hill / Interamericana de España, Madrid, España, 2002. ISBN: 84-481-3620-9.

- Microsoft Education and Cetification, **Supporting Microsoft Windows NT 4.0 Core Tecnologies,** Course # 922, 1997

- José Luis R, Cristina R, **TCP/IP en Windows NT Server,** Editorial RA-MA, Madrid España, 1999.

- Stuart Mc Clure, José Scambray, Gorge Kurtz, **Hackers – Secretos y Soluciones para la Seguridad de Redes,** Editorial Mc Graw Hill / Interamericana de España, S.A.U. ISBN: 84-481-2786-2

- Microsoft, **Windows 2000 Server – Guía de Implantación,** Editorial Mc Graw Hill / Interamericana de España, Edición Profesional, ISBN: 84-481-2845-1.

- Manuel Pons Martorell, **Control de Acceso,** Departamento de Telecomunicaciones, Escuela Universitaria Politécnica de Mataró, 2000.

- Vicente López Camacho, ***Linux Guía de Instalación, Administración, Configuración y Programas de Servidores de Internet e Intranet***, 1ª Mc Graw Hill / Interamericana de España, Madrid, España, 2000

- RADCOM, ***Guía Completa de Protocolos de Comunicación,*** 1ª Edición, Mc Graw Hill / Interamericana de España, Madrid, España, 2002.

INTERNET

- *www.profamilia.org*
- *www.wildpackets.com*
- *www.Equinox.com*
- *www.moxa.com*
- *www.cyclades.com*
- *http://www.netsolutions.com.mx/menu/english/english.shtml*
- *http://www.imagemrio.com.br/subcategoria.asp?NCat=04*
- *http://www.zonalitoral.com/mercadolibre/computacion/modems/index.php*
- *http://es.kelkoo.com/*
- *ttp://www.sitiosargentina.com.ar/mercadolibre/computacion.htm*
- *http://www.optize.es/servlet/navigation?category=8327*
- *http://www.softworld.es/modems/*

Linux

- *www.suse.com*
- *www.redhat.com*
- *www.debian.org*
- *http://linux.corel.com*
- *www.cisco.com*
- *www.hiperlinktech.com*
- *www.mandrakesoft.com*
- *www.etsit.upm.es/~eurielec/linux*
- *www.mulinux.nevalabs.org*
- *www.obelix.umh.es/telematica/practica1.pdf*
- *www.dcc.ufmg.br/~cfmcc/SO_/shell2.pdf*
- *www.biomol1.if.usp.br/msamaral/linux/ apostilalinux-linuxacad.pdf*
- *www.lsd.uam.mx/~oan/ueas/intro_Linux_03l.pdf*
- *www.ec.ucdb.br/~alanari/icomp/linux.PDF*
- *www.sunsite.unam.mx/archivos/linux/linux.pdf*
- *www.tecnet.eluniversal.com/tutoriales/ material/tallerunix.pdf*
- *www.estig.ipbeja.pt/~rmcp/estig/ 2002/2s/p1/trabalhos/tp1_e2.pdf*
- *www.estig.ipbeja.pt/~rmcp/estig/ 2002/2s/p1/trabalhos/tp1_e1.pdf*
- *www.gneher.de/Linux%20Command%20Reference.pdf*
- *www.suse.com/en/business/products/ sles/misc/sles8_en.pdf*
- *www.linux01.gwdg.de/suse/ftp.suse.com/suse/ppc/boot/iSeries/INSTALL.pdf*
- *www.penexchange/misc/ms_exchange_migration.pdf*
- *www.obelix.umh.es/pub/doc/suse/ SuSE-Linux-Basics-8.0.0.1.pdf*
- *www.polyserve.com/pdf/pr_suse.pdf*
- *www.unitedlinux.com/pdfs/suse_certifications.pdf*
- *www.ed.stanford.edu/suse/programs-degrees/ LSTD-FAQ-Release2.4.pdf*
- *www.caribenet.com/pdf/suse_i_en.pdf*
- *www.digicom.it/digisit/com.nsf/ITDepPdfIDX/ SuseDigicom/$file/SuseDigicom.pdf*
- *www.ibm.com/mediumbusiness/venture_development/pdf/*
- *www.linuxnorge.com/distribusjoner/ SuSE/SuSE_81_artikkel.pdf*
- *www.linuxformat.co.uk/archives/LXF34.rev_suse8.pdf*
- *www.theologie.uni-wuerzburg.de/cip/handbuch-7.3.pdf*
- *www.skyrix.com/de/press/releases/ 2001_10_11_eMail_Server_III.pdf*
- *www.pcplus.co.uk/media/pcplus/pdf/177/*
- *www.geocities.com/kane121975/susegtk.pdf*
- *www.gruppointegra.com/suse/emailserver.pdf*
- *www.suse.co.uk/uk/company/schools/sheet.pdf*
- *www.opentrade.com.mx/files/ suse-opentrade_curso-sles_200210cf.pdf*
- *www.linuxuser.co.uk/articles/issue10/lu10-Books.pdf*
- *www.genyosha.de/lnx2002/lnxrouter/ Konfiguration Linux SuSE 62.PDF*
- *www.gaugusch.dhs.org/linux/obsolete/ book-suselinux-reference_de.pdf*
- *www.mirror.usu.edu/mirrors/suse/i386/7.2/ docu/book-suselinux-reference_de.pdf*
- *www.lafacu.com/apuntes/informatica/resel_linux/default.htm*
- *http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html*
- *http://www.pdc.kth.se/heimdal/.*
- *http://web.mit.edu/kerberos/www/*

- *http://web.mit.edu/kerberos/www/dialogue.html*
- *ftp://athena-dist.mit.edu/kerberos/doc/usenix.PS.*
- *http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html*
- *http://www.lns.cornell.edu/public/COMP/krb5/install/install_toc.html*
- *http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/admin_toc.html*
- *http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html*
- *http://www.swcp.com/~jgentry/pers.html*
- *http://www.modemhelp.org*
- *http://www.silug.org/pub/redhat/linux/7.1/emea/doc/RH-DOCS/es/*
- *http://www.hackeralliance.net/linux_download.html*

Windows NT.

- *www.microsoft.com/windows2000/server/howtobuy/pricing/default.asp*
- *www.uv.es./ciuv/cas/vpn.html*
- *www.robertgraham.com/pubs/hacking-dict.htm*
- *www.eurologic.es/conceptos.htm*
- *www.service.real.com/firewall/firewall.html*
- *http://temu.tco.plaza.cl/mg_tec/doc_mg.html*
- *http://www.monografias.com/cgi-bin/search.cgi?query=windows+nt&mh=25&bool=and&substring=0*
- *http://temu.tco.plaza.cl/mg_tec/documentos/winnt/ras.html*
- *http://office.microsoft.com/latam/assistance/2002/articles/AccessEmailFromHome.aspx*
- *http://www.skytel.com.py/html/ras.html*
- *http://www.lafacu.com/apuntes/informatica/cone_wint/default.htm*
- *http://www.informandote.com/jornadasIngWEB/articulos/jiw10.pdf*
- *http/www.nombre.galeon.com*
- *http://enete.fie.us.es*
- *http://www.monografias.com*
- *www.att.com/globalnetwork.*
- *http://www.windowstimag.com/atrasados/1996/04_dic96/pdf/SeguridadWinNT.pdf.*
- *http://h18004.www1.hp.com/products/servers/platforms/index.html*
- *http://h18000.www1.hp.com/products/servers/proliantml350/index_1ghz.html*
- *http://www.geocities.com/SiliconValley/8195/noscs.html#tres*
- *http://temu.tco.plaza.cl/mg_tec/doc_mg.html*
- *http://ccia.ei.uvigo.es/docencia/SSI/VPN.pdf.*

Windows 2000

- *www.microsoft.com/latam/technet/info/edk/SerHome.asp*
- *http://www.w2000mag.com*
- *http://www.microsoft.com/ntserver*
- *http://www.microsoft.com/WINDOWS2000/library/howitworks/security/kerberos.asp.*
- *http://www.microsoft.com/technet/security/authent.asp*
- *http://www.microsoft.com/latam/windows/server/implementacion.htm*

Apéndices

Tablas

Inventario de la Red PROFAMILIA

Oficina Central y Franquicias: Para el Inventario de equipos se tomaron en cuenta cinco características (Maca, capacidad del Procesador, Memoria, Disco Duro y el Sistema Operativo Instalado) que a criterio nuestro son las de mayor importancia para el estudio que estamos realizando, levantado en la oficina central (Plaza el Sol), la Clínicas de Ciudad Jardín, la Clínica de Monseñor Lezcano, las Clínicas Regionales y Franquicias que forman la institución, están asignadas de la siguiente manera:

Tabla A1: Inventario Oficina Central (LAN)

Marca	Procesador	Memoria	Disco duro	S.O
CLON/CENTRUM	PIII 550 MHZ	128 PC-133	10 GB	Win 2000 P
COMPAQ	PIII 733 MHZ	64 PC-133	14 GB	Win98SE
Dirección Financiera				
COMPAQ	PIII 733 MHZ	128 PC-133	14 GB	Win98SE
COMPAQ EVO	PIV 1.8 GHZ	256 PC-133	40 GB	Win98SE
CLON	PIII A 450 MHZ	128 PC-133	6 GB	Win98SE
COMPAQ	PIII 733 MHZ	64 PC-133	14 GB	Win 2000 P
COMPAQ EVO	PIV 1.8 GHZ	256 PC-133	40 GB	Win 2000 P
CLON	PIII A 450 MHZ	128 PC-133	20 GB	Win 2000 P
CLON	PIII 450 MHZ	128 PC-133	6 GB	Win98SE
CLON	PIV 1.8 GHZ	256 PC-133	40 GB	Win 2000 P
COMPAQ	PIII 733 MHZ	128 PC-133	14 GB	Win98SE
CLON	PIV 1.8 GHZ	256 PC-133	40 GB	Win 2000 P
COMPAQ	PII 350 MHZ	64 PC-100	13 GB	Win 2000 P
Dirección Administrativa				
CLON/HURRICANE	PII 400 MHZ	128 PC-133	6 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-100	4 GB	Win98SE
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win98SE
CLON	C4X86 A 66 MHZ	16MB SIMM	500 MB	WIN95
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win 2000 P
UNISYS	PEN 166 MHZ	32 PC-100	2 GB	Win95B
UNISYS	PEN 166 MHZ	32 PC-100	2 GB	Win95B
COMPAQ	AMD K6 450 MHZ	128 PC-133	4 GB	Win 2000 P
COMPAQ	AMDK6/2 450 MHZ	128 PC-133	4 GB	Win98SE
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	WinME
Dirección de Mercadeo Social de Productos y Servicios				
APPLE	G4 450 MHZ	385 MB	20 GB	OSX
IMAC	G3 400 MHZ	128 MB	10 GB	OSIX
COMPAQ	AMD K6/2 450 MHZ	64 PC-100	8 GB	WinME
COMPAQ	PII 350 MHZ	128 PC-133	10 GB	Win 2000 P
DTK	CEL. 300 MHZ	64 PC-100	6 GB	Win 2000 P
DTK	CEL. 300 MHZ	64 PC-100	8 GB	Win95B

DTK	CEL. 300 MHZ	64 PC-133	30 gb	Win98SE
COMPAQ	AMD K6/2 450 MHZ	64 PC-100	8 GB	Win98SE
CLON	CEL. 300 MHZ	64 PC-100	6 GB	Win98SE
CLON	PIII A 550 MHZ	256 PC-133	13 GB	Win 2000 P
Auditoria Interna				
DTK	CEL. 333 MHZ	128 PC-100	10 GB	WinME
CLON	CEL. 366 MHZ	64 PC-100	4 GB	Win98SE
COMPAQ	PII A 350 MZ	128 PC-133	4 GB	Win98SE
Dirección de Planificación y Proyectos				
COMPAQ	PII 350 MHZ	64 PC-100	6 GB	Win95B
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win98SE
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-100	6 GB	Win95B
COMPAQ	P MMX A 233 MHZ	96 PC-100	4 GB	Win98SE
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win98SE
Dirección de Servicios Médicos				
CLON/CENTRUM	PII 400 MHZ	128 PC-100	10 GB	Win 2000 P
CLON	PII 400 MHZ	128 PC-133	6 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-133	4 GB	Win98SE
COMPAQ	PIII A 800 MHZ	256 PC-133	8 GB	Win98SE
COMPAQ	PIII A 733 MHZ	64 PC-133	8 GB	Win98SE
COMPAQ	AMD K6 450 MHZ	128 PC-133	20 GB	Win 2000 P

Tabla A2: Inventario Clínicas De Ciudad Jardín Y Monseñor Lezcano.

Marca	Procesador	Memoria	Disco duro	S.O
Ciudad Jardín				
COMPAQ	PII 350 MHZ	64 PC-100	4.3 GB	WinME
CLON	PIII 550 MHZ	128 PC-133	20 GB	Win98SE
COMPAQ	PII 350 MHZ	128 PC-133	4 GB	Win95B
CLON	PII 400 MHZ	96 PC-100	8 GB	Win98SE
CLON	INTEL/CEL.366	64 PC-100	4 GB	Win98SE
CLON	4X86DX2/66 MHZ	4 MB RAM	230 MB	DOS 5.1
CLON	PII 400 MHZ	96 PC-100	8 GB	Win95B
UNISYS	PENT A 166 MHZ	32 MB	500	Win95B
CLON	4X86DX2/66 MHZ	16 MB	515	Win95A
Monseñor Lezcano				
COMPAQ	AMDK6/2 450 MHZ	64 PC-100	6 GB	Win98SE
CLON	4X86 SX A 33MHZ	4 MB SIMM	512 MB	MSDOS 5.1
DFI	4X86DX2 A 66MHZ	16 MB SIMM	515 MB	Win95A
COMPAQ	AMDK6/2 450 MHZ	128 PC-100	18GB	Win98se

ESTACIONES REMOTAS

Tabla A3: Inventario De Clínicas De Franquicia

Marca	Procesador	Memoria	Disco duro	S.O.
Clínica Franquicia Tipitapa				
CLON/DSD	INTEL/CEL. 550	128 PC-133	13 GB	Win98SE
Clínica Franquicia Sébaco				
CLON/DSD	PIII 550 MHZ	64 PC-100	13 GB	Win98SE
COMPAQ P5363	AMDK6 450 MHz	128 PC-100	18 GB	Win98SE
Clínica Franquicia Somoto				
CLON/DSD	PIII 550 MHZ	64 PC-100	13 GB	Win98SE
Clínica Franquicia Jalapa				
CLON/DSD	PIII 550 MHZ	64 PC-100	13 GB	Win98SE
Clínica Franquicia Río Blanco				
COMPAQ P.5363	AMDK6/2 450 MHZ	64 PC-100	4 GB	Win98SE
Clínica Franquicia Estelí				
CLON/DSD	PIII 550 MHZ	64 PC-100	13 GB	Win98SE
CLON/DSD	PIII 550 MHZ	128 PC-100	10 GB	Win98SE

Tabla A4: Clínicas Centros Regionales

Marca	Procesador	Memoria	Disco duro	S.O.
Clínica Granada				
COMPAQ	PIII 733 MHZ	64 PC-100	14 GB	Win98SE
CLON	INTEL/CEL. 366	64 PC-100	4 GB	Win98
Clínica Rivas				
COMPAQ	P 166 MHZ	16 SIMM	4 GB	Win95A
COMPAQ	PIII 733 MHZ	64 PC-133	15 GB	Win98SE
UNISYS	P 166 MHZ	64 PC-100	5 GB	Win95A
COMPAQ	PII 350 MHZ	64 PC-100	4 GB	Win98SE
Clínica Jinotega				
COMPAQ	PII 350 MHZ	64 PC-100	5 GB	Win98SE
COMPAQ	PIV A 1.8 GHZ	256 PC-133	40 GB	Win98SE
DFI	804X86 DX2 66 MHZ	16 SIMM	500 MB	Win95A
Clínica Matagalpa				
COMPAQ	PIII 733 MHZ	64 PC-100	15 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-100	5 GB	Win98SE
Clínica Chinandega				
COMPAQ	PIII 733 MHZ	128 PC-133	15 GB	Win98SE
CLON	Intel/Cel. 366 MHZ	64 PC-100	3.5 GB	Win95B
COMPAQ	PII 350 MHZ	128 PC-100	4.3 GB	WinME
Clínica Ocotal				
COMPAQ	PII 350 MHZ	64 PC-100	5 GB	Win98
CLON/TRIDENT	804X86 DX2 66 MHZ	8 MB SIMM	385 MB	Win95A
COMPAQ	PIII 733 MHZ	64 PC-133	14 GB	Win98SE
Clínica Boaco				
COMPAQ	PIII 733 MHZ	64 PC-100	14 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-100	5 GB	Win98
Clínica Juigalpa				

COMPAQ	PIII 733 MHZ	64 PC-100	14 GB	Win98SE
COMPAQ	PII 350 MHZ	64 PC-100	5 GB	Win98
Clínica Masaya				
COMPAQ	PII A 350 MHZ	64 PC-100	4 GB	WIN98SE
COMPAQ	PIII A 733 MHZ	64 PC-133	14 GB	WIN98SE

Tabla A5: Disponibilidad de las características de Windows 2000 Server en modo mixto.

Características	Esta disponibles en modo mixto
Relaciones de confianza transitiva para la autenticación Kerberos.	Si, Windows 2000 Server y Windows 2000 profesional usan los servicios Kerberos disponibles en el controlador de Windows 2000.
Unidades organizaciones de Active Director.	Si, pero solo son visibles cuando se utilizan las herramientas de administración de Windows 2000. No se pueden administrar desde los controladores BDC de Windows NT Server 4.0, ni de servidores miembros.
Grupos de seguridad de Active directory.	No, solo están disponibles los grupos locales y globales.
IntelliMirror.	Si, pero solo para computadoras clientes que ejecuten Windows 2000 profesional en un entorno Active directory.
Instalador Windows.	SI.
Arquitectura de memoria de 64 bits.	Si, siempre que el hardware lo permita
Escalabilidad de Active Directory.	Si, pero solo cuando se han actualizado todos los controladores BDC y están ejecutando el servicio de Active Directory. Hay que tener mucho cuidado al utilizar esta característica, porque se siguen pudiendo añadir nuevos controladores BDC de Windows NT mientras el dominio se encuentra en el modo mixto. Esta característica podría ser una parte muy importante del plan de retracción, por lo que no se debería comprometer.
Autenticación Kerberos.	Si, para computadoras Windows 2000 que ejecuten Active Directory.
Microsoft Management Console (MMC).	Si.
Directiva de grupo.	Si, pero solo para computadoras clientes que ejecuten Windows 2000 profesional en un entorno Active Directory.
Configuración y análisis de seguridad.	Si.
Replicación multimaestro de Active Directory.	Si, entre el controlador PDC y los controladores BDC que se hayan actualizado.

Tabla A6: Criterios de seguridad en los sistemas UNIX - Linux

Requisito	Seguridad Discrecional	Accesos Controlados	Seguridad Etiquetada	Protección Estructurada	Dominios de Seguridad	Diseño Verificado
S/Req. Adicionales	Nuevo Criterio	Nuevos Requisitos	S/Req. Adicionales	S/Req. Adicionales	Nuevos Requisitos	S/Req. Adicionales
Reutilización de objetos	No Existe Criterio	Nuevo Criterio.	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales
Dispositivos mononivel/multinivel	No Existe Criterio	No Existe Criterio	Nuevo Criterio	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales
Control de accesos	No Existe Criterio	No Existe Criterio	Nuevo Criterio	Nuevo Criterio	S/Req. Adicionales	S/Req. Adicionales
Etiquetas	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio	S/Req. Adicionales	S/Req. Adicionales
Identificación y autentificación	Nuevo Criterio	Nuevos Requisitos	Nuevos Requisitos	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales
Auditoria	No Existe Criterio	Nuevo Criterio	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	S/Req. Adicionales
Vías fiables	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio	Nuevos Requisitos	S/Req. Adicionales
Arquitectura del sistema	Nuevo Criterio.	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	S/Req. Adicionales
Integridad del sistema	Nuevo Criterio.	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales
Pruebas de seguridad	Nuevo Criterio.	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos
verificación del diseño	No Existe Criterio	No Existe Criterio	Nuevo Criterio	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos
Canales ocultos	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio	Nuevos Requisitos	Nuevos Requisitos
Fácil administración de la fiabilidad	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio	Nuevos Requisitos	S/Req. Adicionales
Gestión de configuración	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio	S/Req. Adicionales	Nuevos Requisitos.
Recuperación segura	No Existe Criterio	No Existe Criterio	No Existe Criterio	No Existe Criterio	No Existe Criterio	S/Req. Adicionales
Distribución segura	No Existe Criterio	No Existe Criterio	No Existe Criterio	No Existe Criterio	No Existe Criterio	Nuevo Criterio
Guía de usuario de seguridad	Nuevo Criterio.	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales	S/Req. Adicionales
Guía de administración de seguridad	Nuevo Criterio.	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	S/Req. Adicionales
Doc de Prueba	Nuevo Criterio.	S/Req. Adicionales	S/Req. Adicionales	Nuevo Criterio	S/Req. Adicionales	Nuevos Requisitos
Doc. de diseño	Nuevo Criterio.	S/Req. Adicionales	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos	Nuevos Requisitos

Tabla A7: Cuadro Comparativo de Módem Externos.

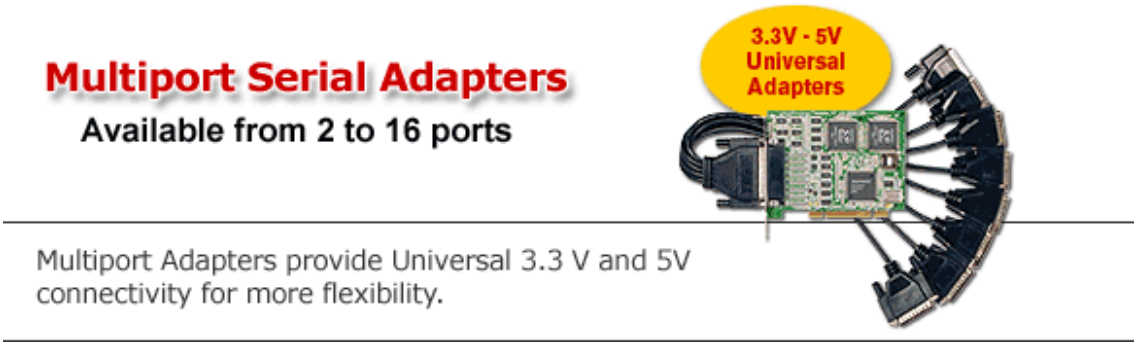
Modelo	*Precio*	*Garantía*	*Puertos*	*Protocolo*	*Velocidades*	*Características*
Trellis VM56KS	$ 243.35	3 Años	Puerto Serial Puerto RJ-11	V.92, V.90, V.80, V.34, V.34+, V.32, V.32bis, V.22, V.22, V.23, V.21	-1200bps (ITU V.22 e Bell 212A). -1200/75bps (ITU V.23) Videotexto. -2400bps (ITU V.22Bis). -4800bps (ITU V.32). -9600bps (ITU V.32). -14400bps (ITU V.32Bis). -28800bps (ITU V.34). -33.600bps (V.34+). -56K (ITU V.90).	Full-Duplex Asíncrono e Analógico. Ajuste automático da velocidades da línea Detección Automática de Voz/Fax. Corrección de error: MNP2-4, V.42/LAP-M. Comprensión de dados: MNP5 (2:1) e V.42Bis (4:1) Programación por software Nivel de Transmisión: 0 a -15 dBm Nivel de Recepción: -43dBm.
D-Link DFM-560EL	$ 95.54	1 Año	Puerto Serial Puerto RJ-11	ITU-T V.90, V.34, .32bis, V.22bis, V.22 Bell 103&212A	- 56K (ITU V.90).	Asíncrono e Analógico. V.42bis y MNP 5 (compresión de datos) V.42 y MNP2-4 (corrección de datos)
U.S. Robotics 0701	$119.00	2 año	Puerto RS232 Puerto RJ11 Puerto D B25	V.92, V.90, V.34, V.32bis, V.32, V.22, V.22bis, V.23, and V.21	28000, 29333, 30666, 32000, 33333, 34666, 36000, 37333, 38666, 40000, 41333, 42666, 44000, 45333, 46666, 48000, 49333, 50666, 52000, 53333, 54666, 56Kbps	Asíncrono e Analógico. V.42/MNP 2-4 (Correcion de Errores) V.42 bis/MNP 5 (Compresión de Datos) V.80 video conferencia
Creative Blaster 7000000002187	$ 67.59	2 Años	Puerto RS232 Puerto RJ-11	V.90, V.92, V.34, V.32bis, V.32, V.23, V.22bis, V.22, V.21; Bell 212A y 103	Velocidad máxima de 56K bps UART de altas prestaciones y velocidad DTE de hasta 115,200 bps	Asíncrono e Analógico. Norma V.80 para H.324 y H.323 Monitorizado de calidad de señal Detección de negociación con servidor Corrección de errores V.42 LAPM y MNP2-4 Compresión de datos V.44, V.42bis y MNP5
Zoom 2949-26-00L	$ 80.10	5 Años	Puerto Serial Puerto RJ-11	V.92, V.90, V.34, V.32bis, V.32, V.22bis, V.22 A/B, V.22, V.23, V.21, V.80/H.324	- 56kbps y 33.6kbps	Asíncrono e Analógico. Full Duplex Compatible con multiplataformas Compresión V.44, V.42bis, MNP5, Control de errores V.42, MNP2-4, Compatible con comandos AT
Genius K964B016	$ 37.68	2 Años	RS-232 Puerto RJ-11	V.92, V.90, V.34bis, V.34, V.32bis, V.32, V.22bis, V.22, V.21, Bell 212A/103 V.27ter, V.29, V.21	56K hasta Transmisión datos 115,200 bps	integra el chipset Agere SV92P (Lucent) Asíncrono e Analógico. cumple la especificación PCI 2.2, Compatible Hayes AT Aprobaciones FCC, CE y CTR-21 Corrección ITU V.42 y MNP2-4 Compresión ITU V.42bis y MNP 5

Tabla A8: Cuadro Comparativo de Adaptadores Multipuertos

Marca	*Equinox*	*Moxa*	*Moxa*	*Cyclom*	*Cyclom*
Modelo	SST- 8P UNIV	C218Turbo Series	CP-168U	Serie "Y"	Serie "Z"
Precio	$ 529.91	$ 680.58	$ 650.00	$ 710.00	Descontinuada
Buffer (I/O)		(512 KB)	Asignada en Bios	1MB	1MB
Slot	PCI - X	32 bits, PCI	32 bits, PCI Univ. I	16 bits ISA / 32 bits PCI	32 bits PCI
Numero puertos	8 Puertos	8 Puertos	8 Puertos	8 puertos	8 puertos
Velocidad por Puerto	920 Kbps Duplex	50bps a 921.6 Kbps	50bps a 230.4Kbps	hasta 115Kbps	Hasta 931.6 Kbps
Soporte	Mayoría Sistemas	Mayoría Sistemas	Mayoría Sistemas	Mayoría Sistemas	Mayoría Sistemas
Interfaz Interna	DB-25, RJ-45 y DB-9	RS-232, RS422/485	DB-62	RS-232 DTE stand. DB-25, 115Kbps RJ-12, 115Kbps RJ-45, DB-25, 115Kbps	16 to 64 RS-232 DTE RJ-45, 921Kbps
Garantía	5 Años	3 Años	3 Años	3 Año	Descontinuada
Características	FCC P. 15 Class A	sistemas	sistemas	Common Asíncrona Manejo de RAS Amb. Multiusuarios FCC Class A and CE	Common Asíncrona Manejo de RAS Amb. Multiusuarios FCC Class A and CE

Adaptadores Multipuertos

Tarjetas Multipuertos Equinox



These intelligent serial I/O adapters use less than 1% system load so servers won't slow down as you run more applications, attach more devices or service more users. SST Multiport Adapters are available in 2, 4, 8 and 16-port configurations. The Equinox line of SST Multiport Adapters deliver the performance and speed you need at a very affordable price. Installation and set up take just a few minutes.

Benefits & Features

- *Universal adapters support a 3.3V (PCI-X) or 5V PCI bus*
- *Connect up to 16 ports to one slot in your server*
- *Supports speeds up to 920 Kbps per port, full duplex*
- *Offloads virtually all serial processing from the host CPU*
- *15,000 volt surge protection on every pin of every port*
- *Includes full modem control signals on all ports (TXD, RXD, CTS, RTS, DSR, DCD, DTR, RI)*
- *Support for most popular operating systems*
- *Easy to install and configure with the "auto-install" feature, no IRQ, I/O ports or memory holes to specify*
- *Includes EquiView Plus management software, as well as SSDIAG for UNIX*
- *DB-25, RJ-45 and DB-9 connectors available*
- *Multiport Adapters have a five-year warranty*

Product Details

The supplied SuperSerial CD includes all drivers, manuals, extensive install/diagnostic help and utilities. Equinox Multiport adapter drivers are included for the following operating systems:

- Windows/95/98/NT/2000/XP
- Linux
- Citrix MetaFrame
- Citrix WinFrame
- Novell AIO
- SCO UNIX
- SCO UnixWare
- Sun Solaris-Intel
- UNIX SVR3
- UNIX SVR4
- MS-DOS

Technical Specifications

Power:	SST-4P/LP UNIV	SST-8P UNIV	SST-16P UNIV
3.3V (mA)	<20	<20	<20
5V (mA)	440	620	1000
12V (mA)	60	110	175
-12V (mA)	-70	-100	-150

Dimensions:	SST-4P/LP UNIV: 5.65"L X 2.50"H X 0.72"W SST-8P UNIV: 5.65"L X 2.50"H X 0.72"W SST-16P UNIV: 5.38"L X 5.00"H X 0.72"W
Weight:	SST-4P/LP UNIV: 1 lb SST-8P UNIV: 1 lb SST-16P UNIV: 2 lb
Speed:	SST-4P/LP UNIV: 920 KBPS SST-8P UNIV: 920 KBPS SST-16P UNIV: 230 KBPS
Modem Control:	Full
Surge Support:	15KV

OS Support:	SST-4P/LP UNIV	SST-8P UNIV	SST-16P UNIV
Windows 9X		•	•
Windows NT	•	•	•
Windows 2000	•	•	•
Windows XP	•	•	•
Citrix	•	•	•
Linux	•	•	•
Novell AIO	•	•	•
OS/2	•	•	•
AIX			
SCO OpenServer	•	•	•
SCO UnixWare	•	•	•
Sun Solaris-Intel	•	•	•

Conformance	FCC P. 15 Class A, CE, UL 60950 3rd Ed., CAN/CSA C22.2 No. 60950-00
Operating Temperature:	0 - 40ºC
Humidity:	10% to 90% (Non-condensing)

Products and Part Numbers

SuperSerial Technology Multiport Adapters from 4 to 16 Ports

4 Port Adapters

SST-4P/LP UNIV - 4 Port Low Profile Universal PCI Adapter (3.3v & 5v), 920 Kbps, (Requires LP fanout cable)	#990449
FO4-DB/LP - 4 Port DB-9 Male Fanout Cable	#690347
FO4-DB/LP - 4 Port DB-25 Male Fanout Cable	#690356
FO4-RJ/LP - 4 Port RJ-45 Female Fanout Cable	#690355

8 Port Adapters

SST-8P UNIV - 8 Port Universal PCI Adapter (3.3v & 5v). 920 Kbps. (Requires fanout cable or CP8)	#990429
FO8-DB - 8 Port DB-25 Male Fanout Cable	#690264
FO8-RJ - 8 Port RJ-45 Fanout Cable	#690265
FO8-DB - 8 Port DB-9 Male Fanout Cable	#690271
CP8-DB - 8 Port DB-25 Connector Panel (For SST-8P)	#990343

16 Port Adapters

SST-16P UNIV - 16 Port Universal PCI Adapter (3.3v & 5v), 230 Kbps, (Requires connector panel)	#990439
CP16-DB - 16 Port DB-25 Connector Panel	#990327
CP16-RJ - 16 Port RJ-45 Connector Panel	#990328
CP16-DB - 16 Port DB-9 Connector Panel	#990422

www.equinox.com

www.Equinox.com

Tarjetas Multipuertos Moxa

MOXA C218Turbo Series

Highest Performance Serial I/O Solution

Overview

MOXA C218Turbo series of multiport serial boards is specifically designed for small but performance demanding applications. With its state-of-the-art ASIC (Application Specific Integrated Circuit), on-board RISC processor (TI TMS320), and large I/O buffer (512 KB), the C218Turbo multiport serial board is a world class I/O serial board. It can maintain a sustained 230.4 Kbps throughput on all eight ports simultaneously while only occupying 5% of the host's processor time*, freeing up more host resources for other tasks. This feature is particularly applicable to fast response demanding industrial control applications, and high speed telecommunication applications.

Features

- ***On board RISC-based processor***
- ***Large I/O buffer (512 KB)***
- ***Delivers the fastest data transmission available, with speeds up to 921.6 Kbps***
- ***Sustained 230 Kbps throughput on all 8 ports simultaneously***
- ***ISA bus also available***
- ***Low repair rate with ASIC design***
- ***Available with optical isolation and surge protection as options***
- ***Works perfectly with all major operating systems***

Benefits

- ***Highest performance to meet all speed-demanding and data intensive communication applications***
- ***Intelligent on-board processor takes a significant load off the host CPU***
- ***Large on-board buffer for high-performance communication***
- ***Compact design size—ideal for high performance, server-based systems***

Specifications

Hardware

Processor	TMS320BC203-57 RISC CPU
I/O controller	16C550C or compatible x 8
Memory	512 KB

Interface

Bus	32-bit, Ver. 2.1 PCI (16-bit ISA also available)
Serial	RS-232, RS-422/485
No. of ports	8

Performance

Speed	50 bps – 921.6 Kbps
Max. No. of ports	32 (4 boards)

Configuration

Parity	None, even, odd, space, mark
Data bits	5, 6, 7, 8
Stop bits	1, 1.5, 2
IRQ	PCI: Assigned by BIOS

OS supported

C218Turbo/PCI	Windows XP, Windows 2000, Windows NT, Windows 95/98/ME, DOS, AT&T UNIX SVR4.2, MITUX SVR4.2, Unix Ware SVR4.2, Unix Ware7 SVR5, SCO Open Server, SCO UNIX, SCO XENIX, Linux 2.0.x (Intel x86), Linux 2.0.x (Alpha), Linux 2.2.x (Intel x86), Linux 2.2.x (Alpha), Linux 2.4.x (Intel x86), QNX 4.2.x

Power and Environment

Power requirements	460 mA max.(+5V), 100 mA max.(+12V), 60 mA max.(-12V)
Operating Temp.	0 – 55°C
Operating Humidity	5 – 95%RH
Storage Temp.	-20 – 85°C
Dimensions	180 x 105 mm (W x D)
Surge protection (Optional)	25 KV ESD for serial port
Optical Isolation (Optional)	500V
Regulatory approvals	FCC, CE

If you need a product with optical isolation, please see the Optional Connectors List below for more information.

Applications

- ***Critical industrial control***
- ***Response demanding monitoring systems***
- ***Embedded industrial machines***
- ***Small Internet/Intranet communication server***
- ***High speed modem/ISDN connectivity***
- ***PC-based routers.***

Ordering Information

C218Turbo/PCI	PCI bus, 8 port intelligent serial board
All items include	• MOXA software CD-ROM: contains drivers and MOXA PComm Lite serial comm development tool • User's Manual

Optional Connectors (choose one per board)

Opt8-M9	8-Port, DB9 Male, RS-232 Connection Box
Opt8-RJ45	8-Port, 8-Pin RJ45, RS-232 Connection Box
Opt8A	8-Port, DB25 Female, RS-232 Connection Box
Opt8S	8-Port, DB25 Female, RS-232 Connection Box w/ Surge Protection
Opt8B	8-Port, DB25 Male, RS-232 Connection Box
Opt8F	8-Port, DB25 Female, RS-422 Connection Box w/ Optical Isolation
Opt8Z	8-Port, DB25 Female, RS-422 Connection Box
Opt8K	8-Port DB25 Female, RS-422/485 Connection Box
CBL-M62M25x8-100 (formerly Opt8C)	8-Port, DB25 Male, RS-232 Connection Cable
CBL-M62M9x8-100 (formerly Opt8D)	8-Port, DB9 Male, RS-232 Connection Cable

CP-168U

8-port RS-232 Communication Board

Overview

MOXA's CP-168 Universal PCI series of multiport serial boards meets the new slot standard for expansion boards that is being rapidly adopted by PC server manufacturers. In addition, CP-168 universal PCI boards will work with both 3.3V and 5V server slots, allowing MOXA boards to be used in virtually any available PC server. The CP-168U series of multiport serial boards offers 8 independent RS-232 serial ports for connecting data acquisition equipment and many other serial devices to the PC and compatible systems.

Features

- ***Supports 8 independent RS-232 serial ports***
- ***Universal PCI bus***
- ***Data flow LED display onboard***
- ***Supports 64 byte FiFo Driver***
- ***Supports Major OS platforms (Windows/Linux)***
- ***Versatile Connection Options***
- ***Embeded 16 KV ESD protection***
- ***50 bps to 230.4 Kbps transmission speed***

Specifications

Communications

Bus Interface	32-bit Universal PCI
Number of Ports	8
Max No. of Boards	4
I/O address/IRQ	PCI BIOS assigned
Comm. Controller	MOXA UART (16C550C compatible)
Baud Rate	50 bps to 230.4 Kbps
Data Bits	5, 6, 7, 8
Stop Bits	1, 1.5, 2
Parity	none, even, odd, space, mark
Data Signal	TxD, RxD, RTS, CTS, DCD, DTR,DSR, GND
Connectors	DB62 Female
Surge Protection	Embedded 16 KV ESD

Environmental

Operating Temperature	0°C to 55°C
Storage Temperature	-20°C to 85°C
Humidity	5 to 95%RH

Mechanical

Dimensions (W x D)	110 x 135 mm (Std. Bracket: 121 mm)

Regulatory Approvals

Regulatory Approvals	CE, FCC

Ordering Information

CP-168U	8-port RS-232 board, Universal PCI bus, 230.4 Kbps, with embedded surge protection (16 KV ESD) *All items include: MOXA Software CD

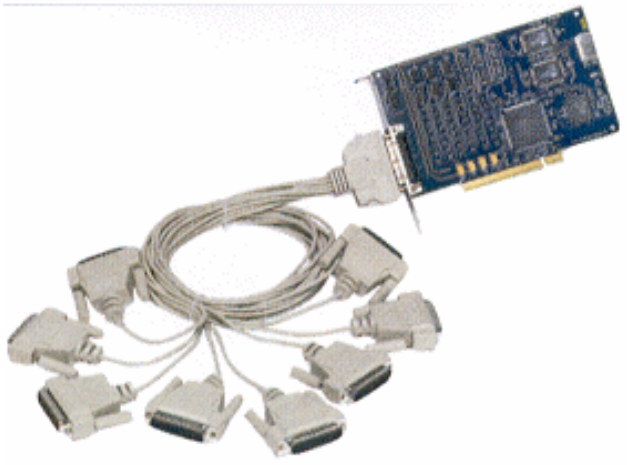
Optional Connectors (choose one per board)

Opt8-M9	8-Port, DB9 Male, RS-232 Connection Box
Opt8-RJ45	8-Port, 8-Pin RJ45, RS-232 Connection Box
Opt8A	8-Port, DB25 Female, RS-232 Connection Box
Opt8S	8-Port, DB25 Female, RS-232 Connection Box w/ Surge Protection
Opt8B	8-Port, DB25 Male, RS-232 Connection Box
Opt8F	8-Port, DB25 Female, RS-422 Connection Box w/ Optical Isolation
Opt8Z	8-Port, DB25 Female, RS-422 Connection Box
Opt8K	8-Port DB25 Female, RS-422/485 Connection Box
CBL-M62M25x8-100 (formerly Opt8C)	8-Port, DB25 Male, RS-232 Connection Cable
CBL-M62M9x8-100 (formerly Opt8D)	8-Port, DB9 Male, RS-232 Connection Cable

www.Moxa.com

Familia de Tarjetas Cyclom

Serie "Y"



El alto rendimiento que tienen los procesadores RISC, que han sido proyectados especialmente para la comunicación de datos, hacen que la familia de tarjetas Cyclom-Y tenga una interfaz multipuerto asíncrona verdaderamente inteligente. Las tarjetas Cyclom-Y proporcionan un alto rendimiento a un costo muy competitivo al compararlas con otras soluciones seriales no inteligentes. Las opciones van de entradas para modelos de 4 puertos a modelos extensibles de hasta 32 puertos por "slot", y están disponibles para interfaces ISA o PCI. Módems, terminales, impresoras, escáneres, colectores de datos, sensores, y puntos de venta son ejemplos de dispositivos seriales que pueden conectarse a las Tarjetas Multipuertos Cyclom-Y.

Aplicaciones

- ***Proveedores de Servicio Internet (ISPs)***
- ***Acceso Remoto***
- ***Sistemas de Tablón de Anuncios (BBS)***
- ***Entornos Multiusuarios***
- ***Automatización Indústrial, Comercial y Doméstica***
- ***Administración de Puerto Consola (Console Port Management)***
- ***Pruebas de Equipos***

Principales Características

- ***4 a 32 puertos RS-232 por tarjeta***
- ***Interfaces ISA o PCI***
- ***Controladores Seriales Integrados y Procesado res RISC***
- ***Conectores DB-25 y RJ-45, internos o externos***
- ***FIFOs internos y una interfaz del hardware muy eficaz de alto rendimiento***
- ***Protección contra Sobrecargas de Energia Eléctrica***
- ***Velocidad de hasta 115Kbps***

Cyclom-Y Especificaciones

Hardware

Procesador Serial:	***CL-CD140 (procesador serial cuadruple)***
Arquitectura Interfaz:	***RISC***

Host:	***16-bit estándar ISA (Yo, Ys, Ye), 32-bit estándar PCI (YoP, YsP, YeP)***
Supresión Sobre tensión:	***Estándar en la mayoría de los modelos***

Intenaces Externas

Cyclom-Yo/YoP:	***Interfaz serial RS-232 OTE, conectar DB-25 (06-9 apenas para Cyclom-4YoP), 115Kbps***
Cyclom-Ys/YsP:	***Interfaz serial RS-232 OTE, conectar RJ-12, 115Kbps***
Cyclom-Ye/YeP:	***Interfaz serial RS-232 OTE, conectar RJ-45 , 115Kbps***

Software

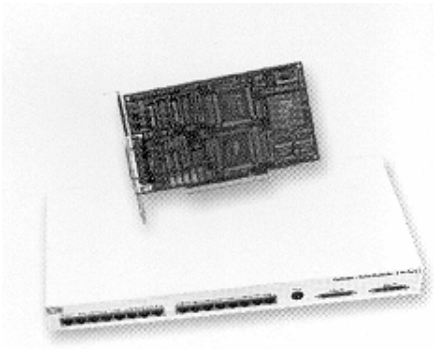
Drivers Soportados: Linux, FreeBSD, BSD/OS Windows (95, 98, NT, 2000, XP)

Alimentación y Aspectos Físicos

Alimentación y Dimensiones:	***Ver sitio Web para obtener el listado completo.***
Temperatura para Operación:	***100 a 440 Celsius (400 a 1120 Fahrenheit)***
Certificaciones:	***FCC Clase B y CE (VoP, Va)*** ***FCC Clase A y CE (demás modelos)***

Cyclom-8Yo:	8 puertos, cable pulpo, conectores 08-25, interfaz ISA
Cyclom-8YoP:	8 puertos, cable pulpo, conectores 08-25, interfaz PCI
Cyclom-8Ys:	8 puertos, conectores RJ-12 incorporados a la tarjeta, interfaz ISA
Cyclom-8YsP:	8 puertos, conectores RJ-12 incorporados a la tarjeta, interfaz PCI
Cyclom-Ye:	16 hasta 32 puertos, tarjeta host interfaz ISA
Cyclom-YeP:	16 hasta 32 puertos, tarjeta host interfaz PCI
Módulo SeriallDB-25:	Caja externa de 16 o 32 puertos DB-25, para la tarjeta host Cyclom Ye o Cyclom YeP
Módulo SeriaVRJ-45:	Caja externa de 16 o 32 puertos RJ-45, para la tarjeta host Cyclom Ye o Cyclom YeP

Serie "Z"



La Tarjeta Serial Multipuerto Cyclades-Ze es la más veloz y más eficiente tarjeta serial del mercado para los usuarios exigentes y aplicaciones especiales. Una única arquitectura con procesador RISC de 32 bits en su CPU (no es un pequeño procesador RISC), con interfaz PCI también de 32 bits (no se trata de una interfaz esclava de 8bits), y 1 MB de memoria auxiliar incorporada en la misma tarjeta. La tarjeta Cyclades-Ze, permite obtener conexiones com un alto rendimiento, que no ocasionarán la más mínima sobrecarga a la CPU.

Aplicaciones

- ***Proveedores de Servicio Internet (ISPs)***
- ***Acceso Remoto***
- ***Sistemas de Tablón de Anuncios (BBS)***
- ***Entornos Multiusuarios***
- ***Automatización Indústrial, Comércial y Doméstica***
- ***Administración de Puerto Consola (Console Port Management)***
- ***Aplicaciones especiales para puertos seriales RS-232***
- ***Pruebas de Equipos***

Principales Características

- ***No ocasionará interrupciones y la más mínima sobrecarga a la CPU***
- ***Puede ser instalado en rack com los prácticos conecto res RJ-45***
- ***Protección contra Sobrecargas de Energía Eléctrica***
- ***Interfaz RS-232, com velocidades de hasta 921.6 Kbps***
- ***Expansible de 16 hasta 64 puertos seriales por slot PCI***
- ***FIFOs internos de 8KB por puerto y una interfaz de hardware muy eficaz de alto rendimiento***

Hardware

CPU:	***IDT3041 (M3000 32-bit RISC)***
Memoria Incorporada:	***1 MB DRAM***
Interfaz Host:	***32-bit estándar PCI***
Supresión de Sobretensión:	***Protección contra sobrecargas de voltaje en las líneas***

Intenaces Externas

Lineas Seriales:	***16 hasta 64 puertos seriales RS-232 DTE, conectores RJ-45, velocidad 921 Kbps***
Cyclom-Ys/YsP:	***Interfaz serial RS-232 OTE, conectar RJ-12, 115Kbps***
Cyclom-Ye/YeP:	***Interfaz serial RS-232 OTE, conectar RJ-45 , 115Kbps***

Software

Drivers Soportados: *Linux, FreeBSD, BSD/OS, Windows (95, 98, NT, 2000, XP) SDK (Software Development Kit) desarrollo de aplicaciones*

Alimentación y Aspectos Físicos

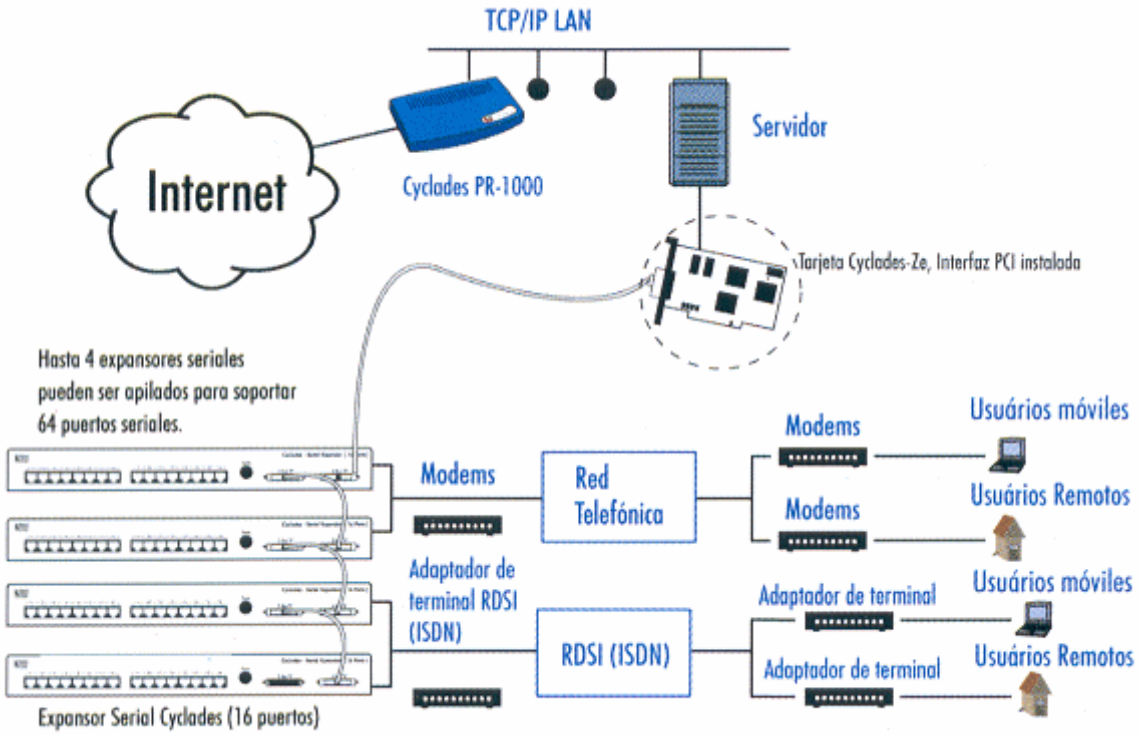
Alimentación: *PCI 4S0mA (+SV) (Tarjeta Host), SOOmA (+12V), 300mA (-12V) (Expansor Serial) Recomendamos fuente de alimentación externa para más que 32 puertos*

Dimensiones: *Tarjeta Host 17.10 cm I 6.73 pulgadas (ancho) 10.60 cm I 4.17, pulgadas (altura). Expansor Serial 43.20 cm / 17 pulgadas (ancho) 21.60 cm / 8.5 pulgadas (profundidad) 4.50 cm / 1.75 pulgadas (altura)*

T. Operación: *10° a 44° Celsius (40° a 112° Fahrenheit)*

Certificaciones: *FCC Clase A y CE*

Cyclom-Z Ejemplos de Aplicación



Cyclom-Y Especificaciones